



PERSEREC

Technical Report 11-01
May 2011

Cyberculture and Personnel Security: Report I – Orientation, Concerns, and Needs

John S. Leggitt
Olga G. Shechter
Northrop Grumman Technical Services

Eric L. Lang
Defense Personnel Security Research Center

**Cyberculture and Personnel Security: Report I – Orientation, Concerns,
and Needs**

John S. Leggitt, Olga G. Shechter—*Northrop Grumman Technical Services*

Eric L. Lang—*Defense Personnel Security Research Center*

Released by – James A. Riedel

BACKGROUND

Computers and related technologies, such as smart phones and video games, are now a common part of everyday life. Many people spend a large portion of their waking hours using and socializing through these devices, forming what is known as a cyberculture. Personnel security investigative and adjudicative standards were developed before these products were widely available; however, cyberculture bears relevance to personnel security due both to the presence of existing security issues and potential effects on psychological outcomes and workplace performance. Although cyberculture has many beneficial effects, this project evaluates how participation can negatively affect personnel security and employee performance. This initial report provides context, outlines presently actionable findings and strategies, highlights some questions that cannot yet be answered, and draws on outside research to guide future research.

HIGHLIGHTS

Information from many sources was examined, including academic research journals, other federal organizations, news reports, and cyber environments, to understand cyber activities relevant to personnel security. Participation is widespread in U.S. society and popular among all age groups. Some cyber activities, such as foreign associations, can be reportable per existing investigative criteria, so procedures should be updated appropriately and promptly. Other topics require research before action is recommended. One concern is how online disinhibition, where people who become more willing to disclose personal information, deceive, or become hostile, affects personnel security. Increased willingness to disclose may amplify the counterintelligence concerns for individuals targeted by hostile parties. There are also many potential negative effects on impulse control, mental health, physical health, and workplace behavior. Future research is intended to further guide policy, workforce awareness, investigations, and adjudications.

REPORT DOCUMENTATION PAGE

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188		
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p>					
1. REPORT DATE: 2011-05-13		2. REPORT TYPE Technical Report 11-01		3. DATES COVERED (From - To) 1994 - May 2011	
4. Cyberculture and Personnel Security: Report I - Orientation, Concerns, and Needs		5a. CONTRACT NUMBER:			
		5b. GRANT NUMBER:			
		5c. PROGRAM ELEMENT NUMBER:			
6. AUTHOR(S): John S. Leggitt, Olga G. Shechter, Eric L. Lang		5d. PROJECT NUMBER:			
		5e. TASK NUMBER:			
		5f. WORK UNIT NUMBER:			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Personnel Security Research Center 20 Ryan Ranch Road, Suite 290 Monterey, CA 93940		8. PERFORMING ORGANIZATION REPORT NUMBER PERSEREC: Technical Report 11-01			
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSORING/MONITOR'S ACRONYM(S)			
		11. SPONSORING/MONITOR'S REPORT NUMBER(S):			
12. DISTRIBUTION/AVAILABILITY STATEMENT: (A) Distribution Unlimited					
13. SUPPLEMENTARY NOTES:					
<p>14. ABSTRACT: Computers and related technologies, such as smart phones and video games, are now a common part of everyday life. Many people spend a large portion of their waking hours using and socializing through these devices, forming what is known as a cyberculture. Personnel security investigative and adjudicative standards were developed before these products were widely available; however, cyberculture bears relevance to personnel security due both to the presence of existing security issues and potential effects on psychological outcomes and workplace performance. Although cyberculture has many beneficial effects, this project evaluates how participation can negatively affect personnel security and employee performance. This initial report provides context, outlines presently actionable findings and strategies, highlights some questions that cannot yet be answered, and draws on outside research to guide future research. Information from many sources was examined, including academic research journals, other federal organizations, news reports, and cyber environments, to understand cyber activities relevant to personnel security. Participation is widespread in U.S. society and popular among all age groups. Some cyber activities, such as foreign associations, can be reportable per existing investigative criteria, so procedures should be updated appropriately and promptly. Other topics require research before action is recommended. One concern is how online disinhibition, where people who become more willing to disclose personal information, deceive, or become hostile, affects personnel security. Increased willingness to disclose may amplify the counterintelligence concerns for individuals targeted by hostile parties. There are also many potential negative effects on impulse control, mental health, physical health, and workplace behavior. Future research is intended to further guide policy, workforce awareness, investigations, and adjudications.</p>					
15. SUBJECT TERMS: Cybersecurity, Internet, Culture, Psychology, Personnel Security, Technology					
16. SECURITY CLASSIFICATION OF: UNCLASSIFIED			17. LIMITATION OF ABSTRACT:	18. NUMBER OF PAGES: 74	19a. NAME OF RESPONSIBLE PERSON: James A. Riedel, Director
a. REPORT: UNCLASSIFIED	b. ABSTRACT: UNCLASSIFIED	c. THIS PAGE: UNCLASSIFIED			19b. TELEPHONE NUMBER (Include area code): 831-583-2800

PREFACE

The Defense Personnel Security Research Center (PERSEREC) Cyberculture and Personnel Security project addresses a looming concern for personnel security: how computer technology and participation in cyber environments is changing which and how information and activities should be evaluated during employee vetting and workforce management. Security-minded organizations are broadly aware that society is being affected by new devices, and are putting policies into place to deal with the constantly changing environment, but the present project takes a different approach by focusing on understanding the long-term implications of these changes. The systemic changes brought about by technology might make obsolete some of the basic assumptions about what needs to be considered during personnel security investigations and adjudications. This research indicates that personnel security may face new behaviors of concern that occur in cyberspace but spill over into real life. In addition, cyberspace expands the range of counterintelligence concerns, such as through activities that increase the disclosure of personal information. The present report is the first in a planned series of related reports. It outlines both the major concerns and the state of knowledge prior to conducting additional research. This information is of interest to all members of the personnel security community, including policy planners, investigators, adjudicators, and employees. In addition, a second independently released report entitled “Cyber Culture and Personnel Security: Report II - Ethnographic Analysis of Second Life,” is based on empirical data and begins to address some of the unknowns.

James A. Riedel
Director

EXECUTIVE SUMMARY

This report is the first in a planned, ongoing series of studies on how computer technology affects society and psychological outcomes, and in turn, requires changes to personnel security policies and practices. Computers and related products, such as smartphones and portable music players, have become common and many people build their lives around them. In doing so, users have formed cybercultures, or societies that depend on computer technology. These can penetrate broadly and deeply into users' lives, be it through social networks (e.g., Facebook, LinkedIn), online multiplayer games (e.g., World of Warcraft, Call of Duty), virtual social environments (e.g., Second Life, IMVU.com), or other products. Social networks change lives by facilitating communication and planning among friends, family, and associates. Online multiplayer games attract users who spend many hours per day, or entire weekends, to interact, compete, and explore. Virtual social environments, such as Second Life, stand out for enabling a wide range of activities among people from across the world. Finally, mobile devices (e.g., smartphones, iPad) allow unique and perhaps deeper changes due to constant access to the Internet and features such as the ability to track physical movement.

While computer technology has had many positive cultural benefits, such as reducing the costs of obtaining information and helping individuals communicate more effectively, the present research is concerned with negative effects relevant to personnel security. The social and psychological impact of computers represents just a portion of the many cybersecurity concerns facing government and industry. Federal cybersecurity interests range from cyber crime, cyber counterintelligence, and cyber terrorism to many additional concerns that fall under the purview of other federal entities. The present project acknowledges these needs, but directs research efforts only to how psychological and cultural changes impact personnel security. Additional information on the general federal cybersecurity context is available through sources such as the President's Comprehensive National Cybersecurity Initiative (CNCI) and documentation of the diverse cyber activities conducted by the Federal Bureau of Investigation (FBI).

It is also well understood that participation in cyber communities can have numerous individual benefits for education, business, entertainment, shopping, social contact, and more. However, this project is concerned with the potential for serious negative effects and spillover into real life. The present report, as the first in the series, outlines the reasons for concern and presents examples of the concerns, provides immediately actionable strategies for managing known risks, reviews relevant scientific literature, and describes topics requiring future research. Cyber activities potentially affect personnel security practices in two main ways: (1) by creating new venues for generating potential problems, such as making it easier for people to cultivate relationships with foreign nationals or engage in illegal activities, and (2) by transforming conventional methods of interpersonal interaction, such that traditional norms and standards used to assess stability, discretion, and judgment are affected.

EXECUTIVE SUMMARY

In general, those cyber activities involving the migration of known issues to new venues present relatively modest cause for deliberation; rather, modernization requires straightforward updates to clarify reporting requirements, investigator training, and adjudicative guidance. In contrast, research is required for topics that have no precise parallels in traditional society. For example, some people now spend many hours per day interacting through computers and text messaging—to the point of being dependent or perhaps addicted—and this may lead them to share information in a fashion that suggests a lack of discretion. Subsequently, the present report is divided into two parts: (1) Orientation and Actionable Strategies, and (2) Scientific Context and Research Guidance. Part I is meant to lay the groundwork for all readers and sketch ways to move forward, while Part II is intended for those who wish to consider the unknowns in detail or plan specific research projects. Later studies seek to provide concrete recommendations in response to important unanswered questions.

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

Cyberculture affects several assumptions about human behavior that are presently made during the personnel security vetting process for what is considered normal, responsible, and even knowable. Specifically, it:

- (1) Often allows for anonymous or depersonalized contact that may dissolve traditional norms and inhibitions.
- (2) Eliminates the need for geographical proximity, allowing for the easy development of relationships across the world.
- (3) Expands the potential for blackmail and exploitation by eliminating the real-world costs and consequences of participation, as users who expect complete anonymity can engage in simulated taboo activities they might not otherwise consider.
- (4) Promotes openness to conversation and sharing personal information as many users join to find chat partners, explore new places, and meet new people.
- (5) Offers practically unlimited opportunities for willing conversation and activity partners, so vulnerable or isolated people may find it difficult to control their impulsive actions and stop participating.
- (6) Creates and increases opportunities for exploitation through collecting personal information for minute daily activities, even among strangers in public spaces.

People today can choose among numerous computer products and environments, and while often superficially distinct, the needs and goals of human interaction are largely similar across the board. From a personnel security standpoint, it does not matter whether a person has, for example, developed a reputation for hacking or

bad business practices in either a social network, a multiplayer game, or in virtual social environment such as Second Life. Because of this, the present report and its immediate follow-up focus on Second Life for research and examples. Second Life is particularly complex and flexible; it allows optional anonymity; and has an established user base. These characteristics were considered desirable for initial research because they permit efficient coverage of the widest range of cyber behaviors of potential security concern. Many cyber activities duplicate behaviors covered by the Adjudicative Guidelines. For example, virtual interaction with foreign nationals relates to Foreign Influence and Foreign Preference concerns, while participation in fantasy sex (e.g., virtual affairs, orgies, rape, or slavery) could be a Sexual Behavior issue if resulting in secretive behaviors that create avenues for blackmail.

Several actionable strategies about the appropriate personnel security response to cyberculture are immediately possible. These include:

- (1) Action should be taken to increase awareness across the personnel security community that cyber activities can be functionally identical to real world activities and can present similar risks. Cyber activities that are reportable per the current Adjudicative Guidelines should be explicitly considered along with real world activities.
- (2) All established cybersecurity topics, such as cyber money laundering, hacking, gang activity, and organized crime, should be systematically reviewed to update personnel security reporting and evaluation guidance.
- (3) No policy, reporting, or enforcement changes should be made to address novel cyber activities that do not derive directly from existing real-world personnel security standards, unless the changes are supported by empirical evidence.
- (4) Personnel security policymakers should address how best to evaluate and manage participation in cyber environments. The core needs are to:
 - (a) Define new and unique cyber topics of potential personnel security interest. Part II presents a range of topics for consideration, and is meant to guide research for this need.
 - (b) Determine the costs and benefits associated with enacting rules to address new topics.

Readers should also consider the findings of an independent PERSEREC research project that seeks to determine appropriate policies and practices for reviewing online activities, or cybervetting. The cybervetting project emphasizes the requirements for and process of collecting information, rather than the present goal of assessing whether given behaviors are of concern. This program contributed to a report released by the International Association of Chiefs of Police (IACP, 2010) that is meant to guide the law enforcement community. Additionally, work is in progress to adapt the findings for national security positions.

PART II: SCIENTIFIC CONTEXT AND RESEARCH GUIDANCE

The second part of the report reviews a range of academic research on how computers and related technologies affect psychological outcomes, and presents examples relevant to personnel security. Prior research suggests at least two major reasons for how computer-mediated relationships affect society, including: (1) online disinhibition – where having technological devices eliminates many cues of face-to-face interaction and can result in exaggerated emotions or behaviors, unrealistic expectations, and a lack of perspective, and (2) impulse control problems or cyber addiction – where technology makes social interaction, games, and other preoccupations constantly available such that they negatively impact real world lives. However, data relevant to personnel security are not available, so these preliminary observations do not yet support changes to policies and practices.

Research on the mental health, physical health, and workplace outcomes of problematic computer use is also reviewed to highlight how maladaptive involvement in cyberculture may affect judgment, reliability, and trustworthiness. Mental health research indicates that maladaptive cyber use is associated with a wide range of emotional problems, such as loneliness, low self-esteem, and withdrawal from family activities. Physical health research indicates that excessive cyber use is associated with loss of sleep (and subsequent performance problems the following day), poor nutrition, and a lack of exercise. Excessive use has even resulted in a number of deaths. Finally, trustworthiness and reliability in the workplace can be affected through lying, rule breaking, and circumventing software that blocks access through personal devices. There have also been a number of cases where government employees, including those with high-level security clearances, have accessed pornography at the workplace. In conjunction, these effects might undermine productivity, expose employers to legal liability, create avenues for blackmail, and negatively impact rules put in place to protect sensitive or classified information.

In looking toward the future, this report sketches research now in progress, specific plans, and other research needs. Report II, as completed in parallel with Report I, examines activities in Second Life in context of the potentially disqualifying behaviors specified in the Adjudicative Guidelines. This study focuses on users who resemble personnel security clearance holders, including being U.S. citizens, holding jobs, and those willing to undergo employment-related background screening. Future research is to use quantitative survey methods to assess the likely prevalence rates of behaviors of concern in a diverse range of cyber environments among individuals who resemble clearance holders and applicants, and also to generate actionable recommendations for investigations, adjudications, and workplace management. Finally, mobile computers and pervasive computing devices (e.g., those in vehicles, embedded in other equipment, or situated in public locations) present unique risks and should receive focused attention.

TABLE OF CONTENTS

INTRODUCTION	1
BACKGROUND AND PROBLEM	1
PROJECT GOALS	4
Cyberculture Research Program	5
Other PERSEREC Cyber Research	5
PART I: ORIENTATION AND ACTIONABLE STRATEGIES	6
AN INCREASINGLY COMPUTERIZED CULTURE	6
Social Networks	7
Online Multiplayer Games	8
Virtual Social Environments	9
Common Characteristics of Popular Cyber Environments	10
Living in a Mobile and Pervasive Cyberculture	13
Summary	15
SECOND LIFE: ONE MANIFESTATION OF CYBERCULTURE	17
OVERVIEW	17
The Second Life Experience	18
Summary	21
KNOWN SECURITY ISSUES AND STRATEGIES	22
False Assumptions of Anonymity and Privacy	22
Cybersecurity, Cyber Crime, and Counterintelligence	23
Sexual Behavior and Personal Conduct	28
Summary	30
PART II: SCIENTIFIC CONTEXT AND RESEARCH GUIDANCE	33
CYBERCULTURE AND PSYCHOLOGY	33
Computer Mediated Relationships and Disinhibition	33
Impulse Control and Cyber Addiction	38
Summary	39
CYBERCULTURE AND MALADAPTIVE SPILLOVER	40
Mental Health Outcomes	40
Physical Health Outcomes	42
Workplace Outcomes	43
Summary	44
GENERAL DISCUSSION	45
Next Steps for the Cyberculture Research Program	45
Conclusions	46
REFERENCES	49

LIST OF TABLES

Table 1 Comparison between Social Networks, Online Multiplayer Games, and Virtual Social Environments	12
--	----

TABLE OF CONTENTS

LIST OF FIGURES

Figure 1 Avatar Appearance Upgrade_____	18
Figure 2 Avatars at a Dance Club _____	20
Figure 3 A Second Life version of the Vietnam Veterans Memorial in Washington, D.C. _____	21
Figure 4 Avatars Playing Games and Conversing in a Version of Moscow's Red Square_____	26
Figure 5 Visa Application Kiosk _____	27

INTRODUCTION

BACKGROUND AND PROBLEM

Computer technology has spread throughout modern society and is often an integral part of everyday life. It facilitates a wide range of necessary and popular activities, such as communication, shopping, finance, news, education, research, games, hobbies, and socializing—and the time people spend using computing devices is increasing. For example, the Kaiser Family Foundation estimates that young people now use entertainment media devices 53 hours a week, which amounts to 7 hours and 38 minutes per day (Rideout, Foehr, & Roberts, 2010). Similarly, a May, 2010 telephone survey found that 40% of those over the age of 50 are very or extremely comfortable using the Internet, and 27% of those over 50 accesses social media sites such as Facebook (AARP, 2010). The present research examines the personnel security implications of a society, or a cyberculture, dependent on computers.

The American Heritage Dictionary of the English Language (2010) defines cyberculture as “The culture arising from the use of computer networks, as for communication, entertainment, work, and business.” Cyberculture has a strong presence in the federal workplace, through the widespread use of personal computers, BlackBerry products, and other devices, and the apparent trend is toward even greater use. For example, the Virtual Government (vGov) initiative of the National Defense University, U.S. Air Force, Homeland Security Department, and Agriculture Department seeks to facilitate collaboration and virtual meetings in the immersive environment of virtual worlds (Lipowicz, 2010). Cyberculture, however, has also drawn personnel security attention and resulted in new personnel security concerns. In April 2009, the Intelligence Advanced Research Projects Activity (IARPA), the research arm of the Office of the Director of National Intelligence (ODNI), unveiled the Reynard Program. Reynard is a multidisciplinary research effort aimed at identifying behavioral indicators in virtual worlds and online multiplayer games that correspond to the real world characteristics of users (Bush, 2009). Similarly, an article in the *Federal Times* warned individuals that their postings and contacts on social networking websites might preclude them from gaining and keeping a security clearance (Rinckey, 2009).

It is crucial to understand that the cultural impact of computers represents only a portion of the many cybersecurity concerns faced by government and industry. The term cybersecurity refers to general security problems associated with computers. Some of the most high-profile federal cybersecurity activities include the President’s Comprehensive National Cybersecurity Initiative (CNCI), the 2009 establishment of the Department of Defense U.S. Cyber Command (USCYBERCOM), and a wide range of cyber programs of the Federal Bureau of Investigation (FBI). However, many important questions do not have immediate answers and are reportedly not being presently addressed. A June, 2010 Government Accountability Office (GAO)

INTRODUCTION

report states that cybersecurity research is crucial but lacks effective oversight and management, and GAO urges prompt federal action. The report argues that without a broad national cybersecurity agenda, research tends to focus on the short term and the needs of individual stakeholders, rather than what may be most important from a national perspective. The present research and other federal actions should be viewed in this context, where unity and the big picture must be a high priority, but also an environment requiring prompt and targeted responses to obvious needs.

The main points of the CNCI are presented below to illustrate where personnel security and cyberculture fit in the more general cybersecurity context. The CNCI is perhaps the most widely known attempt to summarize the range of needs and risks for economic and national security, “designed to help secure the United States in cyberspace.” Some items refer to specific immediate needs (e.g., the deployment of intrusion detection and prevention systems), while others initiatives are open-ended and seemingly in an early stage (e.g., coordinate R&D efforts, define and develop “leap-ahead” activities). Interested parties should refer to the original document for additional details. The three main goals of the CNCI are:

- (1) To establish a front line of defense against today’s immediate threats
- (2) To defend against the full spectrum of threats
- (3) To strengthen the future cybersecurity environment

The 12 supporting initiatives are:

- (1) Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections.
- (2) Deploy an intrusion detection system of sensors across the Federal enterprise.
- (3) Pursue deployment of intrusion prevention systems across the Federal enterprise.
- (4) Coordinate and redirect research and development (R&D) efforts.
- (5) Connect current cyber ops centers to enhance situational awareness.
- (6) Develop and implement a government-wide cyber counterintelligence (a.k.a. CI) plan.
- (7) Increase the security of our classified networks.
- (8) Expand cyber education.
- (9) Define and develop enduring “leap-ahead” technology, strategies, and programs.
- (10) Define and develop enduring deterrence strategies and programs.

- (11) Develop a multi-pronged approach for global supply chain risk management.
- (12) Define the Federal role for extending cybersecurity into critical infrastructure.

Federal cybersecurity measures move forward at different rates between areas, but the FBI provides many examples of clear and concrete progress. The FBI created a cyber division in 2002, has provided cyber training to thousands of its staff, and has been actively working to reduce the risks of cyber terrorism, cyber espionage and cyber crime. In addition, it disseminated more than 1,800 cyber intelligence and cyber analytic products to the Intelligence Community, military, law enforcement, and Department of Homeland Security in Fiscal Year 2009. There are also said to be counterterrorism and counterintelligence efforts that must be discussed in a secure forum (Chabinsky, 2009). Some of the cyber crimes tackled by the FBI include child pornography and the exploitation of children, Internet fraud, and more (Snow, 2010).

Personnel security emphasizes those threats most closely associated with the actions of the cleared workforce. These can originate externally, as when a spy or hacker actively seeks and gathers information, or from inside, as when a trusted employee becomes careless, disgruntled, has sympathy for a foreign government, or seeks to profit from their knowledge. A wide variety of procedures are employed, including requiring that job applicants undergo background investigations and the monitoring of relevant employee behaviors. All together, this system seeks to distinguish members of the workforce who are able to protect sensitive information from those who pose a security risk. Executive Order (E.O.) 12968 describes this goal by stating that eligibility for access to classified information should be granted only to individuals whose character affirmatively indicates trustworthiness, honesty, reliability, discretion, and sound judgment.

All personal characteristics and activities relevant to the safeguarding of sensitive information are of legitimate interest for national security, and many topics are considered when assessing who is to be entrusted with sensitive information. For example, investigations now consider financial history, criminal records, allegiance to the United States, contact or association with citizens of foreign countries, and much more. The emergence of cyberculture raises a new concern because it affects many previous assumptions about personal behavior, as well as if or how cyber behaviors can be investigated. Unfortunately, it is not clear how some cyber activities might relate to traditional interpretations of reliability, trustworthiness, and good judgment. For example, cyber communities often allow anonymous participation, so it is relatively easy to misrepresent oneself and gain access to those in sensitive positions who might otherwise be on guard for exploitation. In 2010, a security consultant created a social network profile for a fictitious young, attractive, “foreign looking” woman who identified herself as a “cyber threat analyst” working for the U.S. Navy. Almost 300 people in the military, security, and intelligence communities established connections with her within a month, including those in senior positions and organizations such as the Joint Chiefs of

INTRODUCTION

Staff, the National Reconnaissance Office, the U.S. Marine Corps, staff of a U.S. congressperson, and major defense contractors. The fictitious woman received invitations to speak at a conference and review a technical paper, and several invited her to apply for jobs (Waterman, 2010).

The greatest unknown from a personnel security standpoint is the potential impact of life-long cyber socialization, or growing up and predominantly interacting through cyberculture, on overall judgment and behavior in the workplace. The concern is that some individuals may internalize cyber world norms in a way that compromises their ability to distinguish between cyber and physical world rules for social interaction and the consequences of actions. The ultimate impact cannot be known until the children growing up today have received security clearances and spent significant time in the workforce, but what is presently known about cyber involvement indicates that over the short term it can harm health, be psychologically maladaptive, and have other negative consequences.

Some of the specific problems now observed among cyber participants include patterns of behavior similar to the addictive and compulsive behaviors described in the Diagnostic and Statistical Manual of Mental Disorders, 4th Ed. (DSM-IV, 1994), and studies report that Internet addicts possess higher levels of depressive symptoms than non-addicts (Morrison & Gore, 2010). Other commonly expressed concerns include social isolation due to reliance on virtual communication, and a lack of discretion in what information is shared with others (e.g., a college student showing pictures of binge drinking episodes on Facebook or a congressman inadvertently disclosing his sensitive whereabouts while traveling through Iraq and Afghanistan [Flaherty, 2009]). Finally, research reviewed in the *Biologist* indicates that increased dependence on technology has negative consequences for sleep, immune system functioning, morbidity, and mortality (Sigman, 2009). In sum, these observations indicate that further study is required, and subsequently the present research project assesses the personnel security implications of widespread cultural reliance on computer technology.

PROJECT GOALS

This report is the first in a planned, ongoing series of studies about personnel security concerns associated with participation in cyberculture, focusing on the psychological outcomes and workplace performance relevant to cleared individuals. This project acknowledges but does not emphasize cybersecurity issues resulting from hostile parties, such as espionage or crime, as they are being addressed by other federal entities. Future studies are intended to use empirical methods to build on what has been learned, and provide a deeper understanding than would be possible otherwise.

The present report provides background information on the personnel security relevance of cyberculture, as based on reviews of academic literature, media reports, websites, and a variety of cyber environments. It introduces core issues,

highlights what can be determined immediately, and outlines examples of topics requiring future research. The document is divided into two parts:

- (1) **Orientation and Actionable Strategies:** An overview of how and why cyberculture impacts personnel security, with the goal of assisting personnel security community stakeholders in moving forward rapidly and efficiently. Several examples are used to illustrate immediate points of action.
- (2) **Scientific Context and Research Guidance:** Material of particular interest to those who seek awareness or who are planning for the future, such as for designing or funding research projects and policy working groups. Examples of a diverse array of cyberculture topics illustrate potential concerns that are not presently actionable.

Cyberculture Research Program

Additional research is presently in progress or has already been completed. A second study, “Cyber Culture and Personnel Security: Report II - Ethnographic Analysis of Second Life,” was conducted in parallel with the present research. It explored potentially problematic behavior patterns that occur in a cyber world. Using qualitative ethnographic research methods, users who chose to participate and who resemble clearance holders (e.g., those who are employed or looking for work, have held, currently hold, or would consider a job requiring a background investigation, are U.S. citizens, etc.) were observed and interviewed. The participants’ cyber behaviors were analyzed in the context of the Adjudicative Guidelines, and an initial framework for understanding behaviors of potential personnel security concern was generated.

Research now in progress seeks to use quantitative methods to assess the prevalence rates for cyber activities of potential concern and generate recommendations for policy and best practices. This is intended to be useful for all personnel security stakeholders, including the cleared workforce, policymakers, investigators, adjudicators, and field management. Additional studies are to be initiated as appropriate.

Other PERSEREC Cyber Research

An independent PERSEREC project seeks to generate appropriate policies and practices for reviewing online activities, or cybervetting. While the (present) cyberculture project studies *behaviors* of apparent personnel security concern, the cybervetting project addresses the legal and technical requirements for, and process of collecting, information to satisfy investigative coverage requirements. The cybervetting project contributed to a report released by the International Association of Chiefs of Police (IACP, 2010) that is meant to guide vetting in the law enforcement community. Additionally, work is in progress to adapt the findings for national security positions.

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

AN INCREASINGLY COMPUTERIZED CULTURE

Computer technology has so many uses and so much flexibility that it regularly changes how people perform common activities. Many of these changes affect how people go about their business, but are ultimately unremarkable from a personnel security perspective. Examples include using email instead of a telephone, using online banking instead of sending checks through the mail, looking up information on the web instead of using an encyclopedia or a telephone book, and comparison shopping through a website rather than with catalogs or by visiting local stores. Instead, the important questions are if and how dependence on computer technology might affect thinking and socialization, whereby presently accepted personnel security standards no longer effectively differentiate between behaviors that pose a risk to controlled information, nor between reliable and unreliable employees. People who grow up and spend the bulk of their waking hours surrounded by such technology may conduct their personal lives in different ways, may behave differently in the workplace, and take a different approach to tasks or respond differently to direction from management.

Society seemingly changes in conjunction with computer technologies. A New York Times story argues that technological generation gaps are now occurring at a rapid pace, such that there are differences in the cyber activities of young children, those in their teens, their twenties, their thirties, and older (Stone, 2010). A Computerworld.com essay notes that those currently between the ages of 20 and 60 are the only people in human history to communicate with traditional one-to-one (e.g., letters, telephone) and one-to-many (e.g., radio, newspaper, television) methods, as well as the new any-to-any method of social networking (Elgan, 2010). Subrahmanyam and Greenfield (2008) outline how adolescents growing up today face a broad array of new technologies, and that many basic questions have not been studied. They also point out that contemporary social networking applications have made conclusions about the Internet from just 10 or 15 years ago obsolete. Subsequently, to understand technologies with the greatest potential for affecting cognition, socialization, and workplace behavior, the present research seeks those involving the greatest changes relative to noncomputerized cultures.

Three current implementations of cyberculture stand out as being widespread and popular, having participants who display strong and persistent interest, and for providing ways to substantially change social, hobby, and other aspects of personal lives. They include: (1) social networks (e.g., Facebook, MySpace), (2) online multiplayer games (e.g., World of Warcraft, Everquest), and (3) virtual social environments (e.g., Second Life, IMVU). These are now common across American society, and adults frequently participate, rather than just teenagers and college students. Social network participation is expanding in all age groups. For example, a *2010 Facebook Demographics and Statistics Report* showed that approximately

two thirds of all Facebook users were adults 25 and older (Corbett, 2010). The fastest growing Facebook demographics were adults 35-54 years old and adults aged 55+. The 35-54 demographic grew by 25.2% between January and June 2010, while the 55+ demographic grew 35.3% in the same period. An August 2010 report (Pew Research Center) indicates that social networking among those over 50 years of age increased from 22% to 42% in the prior year, and 26% of those over 65 now use social networks. Similarly, video games are estimated to be played in 65% of American households and the average gamer is now 35 years old (Weaver et al., 2009). Statistics reported by Linden Lab in 2008 show that 84% of Second Life users are 25 and older, and that adults aged 25-34 make-up the largest demographic of all Second Life users (34%). Each type is briefly introduced below, and then they are discussed together to highlight universal commonalities. Finally, all cyber activities are affected by mobile devices with unique security concerns, and mobile technology itself has the potential to more thoroughly change society.

Social Networks

In the simplest sense, an online social network provides an efficient way of sharing and obtaining personal information. Some of the most widely known and popular social networks include Facebook, MySpace, and LinkedIn. They have become a common method for maintaining social contact with friends and family, as well as for finding employment and other individuals with similar interests. The Nielsen Report (2010) states that three fourths of those who go online across the world now use social media websites (which also include blogs, Wikipedia, and YouTube), that 22% of all time spent online occurs at these sites, and that usage has been rapidly increasing. Social networks typically combine general information about a person, the ability to send messages, immediate updates on current activities, and a way of organizing topic-specific interests, photographs, hobbies, or games. They represent a significant shift from previous methods of social contact by efficiently bringing together a wide range of people and personal information in one place. As the information in social networks is primarily about real people, the main decisions facing users are whether to share the information at all, and how to control the information available to each circle of associates (e.g., family vs. business associates vs. friends).

Social networks raise concerns for employers because potential or current employees can exercise poor judgment with the activities, associates, and information they share about themselves. The longer-term question is how social networks might affect cultural standards for privacy. An Internet security firm surveyed 2,200 mothers across 10 industrialized countries with Internet access and children aged 2 or younger. They found that the average child acquires an online presence at 6 months and 81% have a digital footprint (e.g., photos, pre-birth scans, email addresses, etc.) by age 2 (Smith, J., 2010). Furthermore, the author argues that people under 20 years of age now naturally share information through Facebook, as for them it resembles chatting at the water cooler with colleagues, so

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

it must eventually be permitted in the workplace. In addition, the founder and CEO of Facebook, Mark Zuckerberg, has made several highly controversial statements and management decisions on privacy, such as saying that people now care less about keeping information private than previous generations (Kirkpatrick, 2010).

To the extent that society is changing in the direction of sharing more information, social networks may present additional challenges for the protection of private, proprietary, and classified information. The consequences of sharing are potentially much more damaging than in the past, for material can now be immediately transmitted across the world and stored indefinitely. As described in the introduction, a security consultant demonstrated that many personnel security professionals quickly befriended an attractive but fraudulent peer on social networks (Waterman, 2010). Similarly, Facebook progressively relaxed its default privacy settings over the last several years, moving from sharing only with friends, schools, and personal networks to now sharing almost all information with anyone across the Internet (McKeon, 2010). To illustrate how such data might be exploited, another security consultant used software to read and compile the public information of 171 million Facebook users (one third of the 2010 total of 500 million), and made it available for downloading (Paul, 2010).

Online Multiplayer Games

Online multiplayer games, which are played through a wide variety of computer and video game devices (e.g., desktops, notebooks, Playstation, Xbox, iPhone, etc.), provide a way of matching people for competition, social interaction, group participation, or cooperation to achieve a common objective. Multiplayer games can be as basic as finding a partner for checkers, or involve thousands of simultaneous players in near photorealistic virtual environments that simulate a city, kingdom, racetrack, battlefield, etc. Many popular games (e.g., Call of Duty, Halo, Quake, Doom, etc.) focus on virtual armed combat between individuals or groups. In addition, online games often incorporate complex stories that parallel an epic film or lengthy novel, and use a form of social networking through guilds or teams (e.g., World of Warcraft, Everquest, etc.).

While computer and video games have often been criticized for promoting or desensitizing users to violence (Carnagey, Anderson, & Bushman, 2007; Dill & Dill, 1998), they also have military purposes. For example, since 2002, the U.S. Department of Defense (DoD) has been using a game called America's Army as a recruitment and training tool (White, 2005; AmericasArmy.com, 2010). Similarly, pilots stationed near Las Vegas use a computerized remote control system that strongly resembles flight simulator games to fly unmanned aircraft over Afghanistan and Iraq that fire real weapons and result in real deaths (Frontline, 2009). These examples show that game technology clearly has useful roles in the military, so the functional benefits of games must be distinguished from any unwanted negative effects.

Of the greatest interest for the present research, online multiplayer games change traditional society by eliminating many real world limitations characteristic of competition and team interaction. For example, before computers were available, an individual desiring competition might have visited a community center, organized a poker game, played chess by mail, or joined a local baseball league. Today, however, a person can find instant matches through thousands of products and with millions of players. Competitors can be found any time of the day, during bad weather, and when no one nearby shares similar interests. The most apparent security-relevant consequence is that the all-you-can-eat atmosphere may promote acting on impulse or result in clinical addiction among susceptible individuals. Research indicates that some game designs are consistent with a reward system that promotes greater and longer use, as developers profit through ongoing user subscriptions (Ducheneaut, Yee, Nickell, & Moore, 2006). Furthermore, the social components of online multiplayer games parallel social networks, and social networks also include games (e.g., FarmVille, CityVille, Café World, FrontierVille, Mafia Wars, etc.). As socially networked games tend to be more popular among female players and those outside the 18-34 age group, they expand the concerns for personnel security and the workplace beyond those traditionally recognized for young males who play games (Gross, 2010).

Virtual Social Environments

A 3D virtual environment is a simulated physical place, be it real or imaginary, created through computers. A user or users can “be” in that place through a computer display, most often using a first-person “through the eyes” or a third-person “over the shoulder” view. Many games employ virtual environments, but virtual environments have other purposes too. Second Life is probably the most well known virtual social environment, and it has a much broader scope than any game. It was released by Linden Lab in 2003 and has experienced many changes over subsequent years (Clark, 2010). While it visually resembles a game, it is meant to provide a way of sharing user-created content, locations, and experiences rather than be a game per se. Users choose what to do and can buy virtual real estate to build what they wish, so, due to this flexibility, it may exhibit the widest range of activities of any virtual environment. Within this flexible design, it shares many aspects of both social networks and multiplayer games. Going beyond games, Second Life users have no explicit goals, but they can play games if desired. Going beyond social networks, Second Life users need not share their name but can choose to reveal their identity and interests, as well as maintain a list of associates.

Between 2005 and 2008, Second Life received widespread media attention and experienced rapid changes due to well-funded experimentation by businesses, individuals, and organizations who perceived it as an opportunity for being at the forefront of the cultural changes enabled by computer networks. As described below, news stories from that era discuss Second Life’s growing popularity, all that was attempted with the minimal restrictions Linden Lab placed on virtual real

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

estate, and the things that failed. The optimism associated with trying new ideas led to a rushed atmosphere and generous spending relative to the rewards, much like the 1990s-2000s dot-com, real estate, and financial bubbles. An influential magazine cover story described how a single person owned virtual real estate worth \$250,000 U.S., and made money from virtual rentals and sales (Businessweek, 2006). Corporations including Best Buy, Cisco, Reuters, Pontiac, Dell, H&R Block, and more created elaborate in-world locations (Brandon, 2007), but interest quickly declined because users simply did not visit corporate sites (Semuels, 2007). In-world banking and gambling also rose in popularity, but were then banned by Linden Lab due to various difficulties and real-world laws (Reuters, 2007; Terdiman, 2008). IBM pushed for the use of virtual worlds in corporate environments, such as remote meetings and conferences (Brodkin, 2008). Finally, as early as 2007, more than 300 real-world universities established a presence in Second Life, and used it for remote teaching and course supplementation (Sussman, 2007); however, educational institution interest may now have shifted or expanded to other virtual worlds (Young, 2010).

In the aftermath of the publicity and many failed attempts at commercialization, Second Life now has a lower profile but apparently a strong business niche. Statistics show that usage is increasing and is at an all time high, with 826,214 monthly unique logins for repeat visitors as of March 2010 (Nino, 2010; Hopkins, 2010). Similarly, user-to-user financial transactions for 2009 were worth \$567 million U.S. (Rosenwald, 2010) and \$160 million U.S. in the first quarter of 2010, which are also all time highs (Hopkins, 2010). Although Linden Lab announced some layoffs in 2010 associated with consolidation efforts (Woollacott, 2010), virtual social environments such as Second Life are likely to be popular for the foreseeable future. Examples from Second Life are used throughout the present report because it makes a wide range of activities possible, and because the second report on cyberculture focused on its users.

Common Characteristics of Popular Cyber Environments

Different cyber environments often provide similar experiences to their users, as all of them facilitate social activities through computer technology rather than face-to-face interaction. The examples presented above are merely snapshots, for there is no single version of cyberculture and each implementation constantly changes. In fact, many environments are tending to adopt the features and capabilities of each other and become ever more similar in the process. In many ways it is pointless to draw clear lines between social networks, multiplayer online games, and virtual social environments. Facebook games such as FarmVille, CityVille, and Mafia Wars give players an advantage for linking to friends who also play, and linking is necessary for advancement (Chen, 2009; Gross, 2010; Mafiawarstips.com, 2010). World of Warcraft players must eventually join social guilds or teams to complete difficult challenges and make progress in the game (Ducheneaut, et al., 2006), and the CEO of Activision Publishing said that the online game Call of Duty “has in

many ways become one of the world's most engaged social networks” (Albanesius, 2010). Apple announced a social network for game players, whereby users of their smartphones can find opponents, collect achievements, and see competitive rankings on scoreboards (Steinberg, 2010). Finally, Linden Lab plans to move Second Life to web browser software, mobile devices, and extend it for integration with social networks such as Facebook (Woollacott, 2010).

Many examples of cyberculture largely overlap, seemingly because activities are popular only when interesting or useful from an ordinary human standpoint. Regardless of technology, people continue to have the same needs and goals in life, including finding companionship, entertainment, or satisfying employment, and building families. As such, popular cyber environments succeed by touching on these interests and naturally tend to be similar. The characteristics of each type of environment are presented in Table 1 (page 12), and their commonalities are summarized in the remainder of this section. Table 1 also outlines the most apparent potential security risks for each type of cyber environment. For those readers who prefer a narrative description, the captions below the table provide similar information.

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

Table 1
Comparison between Social Networks, Online Multiplayer Games, and Virtual Social Environments

	Social Networks	Online Multiplayer Games	Virtual Social Environments
Major Goals	Share personal information, interests, and activities with family, friends, and associates. Also used for games, shopping, advertising, etc.	Compete against or cooperate with others to achieve a common goal, often including a fantasy element; social interaction; buying and selling of game objects.	Social interaction; fantasy and role-play; shopping; virtual art and tourism; games; music; video; design; business meetings; education.
Level of Privacy	Low – the primary purpose is to share real-life information.	High or low – chosen by each user.	High or low – chosen by each user.
Breadth of Activities and Choices Available	High – many users, groups, and activities. Because users' identities are generally known, participation often involves impression management ¹ or discretion.	Low to moderate – games are typically designed to have clear competitive objectives, controls to prevent cheating, and ways to manage user interaction.	High – designed for flexibility and comprehensive options, plus optional anonymity eliminates societal barriers to experimentation with alternate lifestyles.
Major Topics of Apparent Relevance to Personnel Security and Real Life Spillover	1. Lack of discretion about the information revealed may reflect poorly on judgment and open the door to identity theft or exploitation. 2. Clinical addiction or impulse control disorders. 3. Easy communication with foreign nationals. 4. Hacking.	1. Clinical addiction or impulse control disorders, amplified by designs whereby developers profit by promoting heavy and long-term use. 2. Activities such as photorealistic simulated violence may blur the fantasy vs. reality boundary. 3. Excessive spending to support a hobby. 4. Easy communication with foreign nationals. 5. Hacking.	1. Lack of discretion coupled with engagement in simulated taboo activities. 2. Clinical addiction or impulse control disorders. 3. Easy communication with foreign nationals. 4. Illegal activities such as gambling or simulated pedophilia. 5. Excessive fantasizing may blur the boundary with reality. 6. Excessive spending to support a hobby. 7. Hacking.

- *Major Goals:* Social interaction is universally popular, and while many environments offer a wide range of activities, each user chooses what to do. Virtual social environments generally offer the widest variety of potential goals and are also the most flexible, as the developer does not dictate users' goals. Note that social networks are rapidly gaining new capabilities too.

¹ It is possible to create independent or fictitious profiles on many social networks, such as for privacy when engaging in activities that may be criticized, keeping circles of associates apart, manipulation or social engineering, etc.

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

- *Level of Privacy:* The main difference among the types is that social networks are designed to share personal information, so users must reveal information to fully and effectively participate, while identity is often a secondary consideration or irrelevant in the other cyber environments.
- *Breadth of Activities and Choices Available:* Online multiplayer games stand out as being more goal-oriented and less flexible than social networks or virtual social environments. Games are designed primarily for competition and achievement whereas social networks and virtual social environments are intended for diverse activities.
- *Major Topics of Apparent Relevance to Personnel Security and Real-Life Spillover:* All three types share the potential for excessive use or spending, hacking, and social engineering or exploitation by hostile parties. In addition:
 - (1) Social networks, in facilitating real-life relationships, present a particular concern as tools for collecting, organizing, and storing evidence suggesting poor judgment and a lack of discretion. Due to weak privacy restrictions, people can also be victimized by the decisions of associates (e.g., a friend posting detrimental photos), and hostile parties (e.g., foreign governments) might easily profile and target those likely to possess valuable information.
 - (2) Online multiplayer games usually involve a limited range of competitive goals, but if designed to encourage more and longer play, vulnerable participants may be more likely to experience impulse control problems or become clinically addicted. Games have a strong fantasy component, so certain individuals or heavy users may confuse real life and cyber rules. Note that some social network games inform real-life “friends” of activities that may suggest overuse, and subsequently reveal poor judgment.
 - (3) Virtual social environments present the broadest range of concerns because of their flexibility. The potential concerns include all those found with social networks and online multiplayer games. However, with optional anonymity, users may be more open about sharing private information, resulting in greater vulnerabilities if a real identity becomes known.

Living in a Mobile and Pervasive Cyberculture

Cyberculture involves truly conducting one’s life through computer technology, and this means that numerous aspects of daily life can be affected. The discussion has considered how cyber activities shape and supplant a wide range of real world activities, but the impact extends well beyond desktop and notebook computers, and beyond sitting passively in chairs. Most notably, people participate through smartphones and pocket computers, but also through pervasive computing devices, such as those encountered in vehicles, appliances, kiosks, televisions, alarm clocks, or anything else with Internet access. In fact, nontraditional computers both

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

duplicate traditional concerns and result in unique security concerns. They more fully illustrate what it really means to live today in a cyberculture.

Having easy and continuous access to computers opens the door to two major outcomes. First, it increases the potential for outright dependence, whereby people literally cannot function without them. In some sense this is obvious and unremarkable, as many professionals today would be unable to function without cell phones or smartphones, but the impact is broadening over time. Dependence is discussed more generally in Part II of the present report, as firm conclusions require further research. Second, mobile computers have the same basic characteristics of all computers, so they “attach” these to each and every daily activity. On the positive side, users gain the power to obtain detailed information about any topic at any time, but on the negative side people carry with them known computer security concerns, including hacking, social engineering, and additional pathways for exploitation. As phones with features such as picture taking, Internet access, email, instant messaging, games, and music are now commonly used by Americans (Smith, A., 2010), such products are of immediate interest.

Mobile and pervasive computing bring traditional security concerns to more and more places in daily life. Location-based services integrate real-world places (i.e., physical locations/GPS coordinates) with Internet information to help users be more knowledgeable and efficient as they move about the world. Some of the more well-known products include Foursquare (social networking, exploration), Gowalla (social networking, exploration), Urbanspoon (restaurant finder), and Yelp (restaurant and business finder, user reviews). While in the past a person looking for a good restaurant might have asked at a hotel or gas station, or simply wandered around looking for a crowd, users today can search the surrounding area for a type of food, for those with the best reviews, or for those open at a given time. These products can be enormously useful, but it is effectively impossible to ensure that the information provided is accurate or being handled ethically. For example, Yelp has been sued for extortion and fraud, with claims that Yelp’s sales staff promised to remove negative business reviews only if the businesses paid to advertise. At the time of writing, Yelp has denied the allegations (Ali, 2010). Theoretically, a business such as this might manipulate independent companies, or be a front for a hostile entity that tracks user movement, identifies individuals with valuable information, and facilitates the recruitment of agents.

Additional topics of security interest arise from the information that users share and collect on their own. For example, one’s GPS location can be combined with photos taken by a smartphone to obtain information about landmarks of interest to tourists, find the identity of artwork, obtain additional product information in a store (Google, 2010), and even the name and personal details of a stranger who has a photo in the Facebook database (Chang, 2010). As long a photo can be taken and the Internet searched, there is no limit to what a person could learn about those around them. Users could find people who are looking for a partner, are a friend-of-a-friend, share a common hobby, share religious beliefs, share a political ideology,

or have other characteristic of interest (Ionescu, 2010). An example of the impact comes from a Twitter user in South Africa who updates 6,000 followers about police roadblocks and speed traps so motorists can avoid fines and delay. While some of his followers view him as a hero, the police considered charging him with obstructing justice (BBC News, 2010). The chief security concern is that, in the process of increasing users capabilities, they also increase the power of other individuals to track and target people for exploitation. In fact, both the U.S. Air Force and U.S. Army have issued warnings about how location sharing can assist hostile forces (Diana, 2010)

Information sharing among mobile device users has transformed how many social and political events are organized, and also how the participants interact with other segments of society. A flash mob is a quickly organized group that meets in a public location for any number of purposes (Kelkar, 2010), but often for performance art or to create a social event. For example, Star Wars fans in England organized one at a shopping mall to conduct a mass light saber fight (Zani, 2010), a group of 70 Ohio State University students started singing and dancing in unison (Henthorn, 2010), and a flash mob snowball fight in Philadelphia ended in vandalism and violence (Sheridan, 2010). Several foreign governments have suppressed information resources to control political opposition, which clearly demonstrates a deep impact. In early 2011, social media were a factor in driving the Tunisian leader from the country, and shortly thereafter political flash mobs were organized to protest the Egyptian government (Timpane, 2011). The Egyptian government responded by cutting off virtually all Internet and mobile communication, and this was much more comprehensive than similar government shutdowns of communication by Iran in 2009 and Myanmar in 2007 (El Gazzar, Vitorovich, & Bender, 2011).

The most important generalization about mobile and pervasive computing is that everyone is affected, regardless of whether one chooses to participate. This is because strangers can access vast information resources and have a far greater impact than in past generations. The ability to learn personal information now extends beyond friends and associates to private businesses, hostile or illegitimate governments, and literally anyone with a mobile device. The mere presence of computing devices in public locations combines all long-established real world security risks with those made possible by the web, and voluntary participants may differ from nonparticipants for expectations of privacy and discretion.

Summary

Cyberculture alters several basic assumptions about human behavior that are presently made during the personnel security vetting process for what is considered normal, responsible, and even knowable. The current investigative standards and Adjudicative Guidelines were developed when cyberculture was restricted to small segments of society and an afterthought. Now that computer-mediated culture has entered the mainstream, regular participation should be expected across the

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

cleared population. The core need going forward is to recognize what stays the same as computers enter the picture versus what changes. In sum, cyberculture:

- (1) Often allows for anonymous or depersonalized contact that may dissolve traditional norms and inhibitions.
- (2) Eliminates the need for geographical proximity, allowing for the easy development of relationships across the world.
- (3) Expands the potential for blackmail and exploitation by eliminating the real-world costs and consequences of participation, as users who expect complete anonymity can engage in simulated taboo activities they might not otherwise consider.
- (4) Promotes openness to conversation and sharing personal information as many users join to find chat partners, explore new places, and meet new people.
- (5) Offers practically unlimited opportunities for willing conversation and activity partners, so vulnerable or isolated people may find it difficult to control their impulsive actions and stop participating.
- (6) Creates and increases opportunities for exploitation through collecting personal information for minute daily activities, even among strangers in public spaces.

Personnel security investigations and workforce management have long considered information from real-world friends, family, and associates, as well as traceable activities maintained by external parties, such as crime reports and financial records. The emergence of cyberculture adds to what may be important to consider, and the inherent differences can require the rethinking of policies or additional research. Some of the resulting questions include:

- (1) How to determine and evaluate when cyber activities materially and adversely spill over to real-life relationships, attitudes, and practices.
- (2) Whether background investigations can and should consider fantasy activities that may intentionally blur legal boundaries.
- (3) Whether any cyber activity performed with a reasonable expectation of anonymity needs to be reported or should be considered.
- (4) Whether anonymous activities in certain cyber environments can be effectively investigated or confirmed.

None of these questions were answerable on the basis of previous research or accepted standards and practices. Those topics that can be addressed are discussed at the end of Part I, while Part II and planned follow-up research seek to establish more practical and specific recommendations for the personnel security community.

SECOND LIFE: ONE MANIFESTATION OF CYBERCULTURE

OVERVIEW

People today have millions of cyber communities to choose among. Many are simple and limited, such as special interest blogs or discussion groups (e.g., finance, movies, politics, automobiles, music, etc.) that present news items and allow readers to comment using a real or fictitious screen name, while others impact a broad range of interests and activities. The discussion above outlined a range of complex types, but as can be easily confirmed through first-hand experience, many activities and social patterns tend to be similar across communities. The choice of which community to join, and which ones become enduring and important to a user, depend on factors such as personal hobbies and interests, the desire to explore, the presence of or recruitment by friends and family, news events that have sparked curiosity, and more.

Second Life was selected for initial research because it provides an efficient way to observe many topics relevant to personnel security. A wide range of activities are possible, including classes from real colleges, business meetings, virtual tourism, buying and selling virtual goods, socializing, and special interest clubs; it has a well-established user base, which is beneficial for assessing the long-term impact of participation; its graphics make it possible to visualize the reasons for concern; and its optional anonymity increases the chances of encountering users who experiment with activities that could negatively impact their real lives. Anonymous users, such as people with fictitious social network identities, have no incentive for maintaining a reputation or avoiding activities that would be frowned upon by colleagues, friends, or family. All in all, Second Life provides a good way to illustrate the broad impact of a cyber social hub.

An important question resulting from the choice of Second Life revolves around how typical it is versus other cyber communities. As discussed above, the complexity, fluidity, and diversity of modern products largely prevent absolute conclusions about specific environments or users. Note that Facebook went from serving the college population to the mainstream in just a few years, and as happened with MySpace, it may also decline in influence as new products become available. Similarly, people typically use multiple providers for distinct activities, ranging from LinkedIn for business contacts, Facebook for friends and family, ChatRoulette for meeting strangers, and pornography websites for video sex. From a personnel security standpoint, the bottom line consideration is whether any activity poses a risk to protected information such that it requires reporting and adjudication. However, future research may help guide the allocation of resources by estimating the degree of concern posed by specific activities and environments. See Part II for potential research topics.

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

The Second Life Experience

The authors created free Second Life personal accounts to better understand the capabilities of the virtual world and to determine if and how it might be studied. This was necessary to assess the potential for further research, and it also served to guide the formal ethnography of Second Life described in Report II. The present report describes Second Life and outlines examples of personnel security concerns, whereas Report II provides detailed findings on the activities of those who agreed to participate in the research. The images in this report were obtained using the integrated screenshot capabilities of the viewer software. All contact with other users was anonymous and occurred in public locations (i.e., akin to walking down a street and snapping pictures). The images provide a feel for what is present and how people interact, but only begin to scratch the surface of the content. Hundreds of thousands of additional images posted by Second Life users are publicly available at Flickr.com and other photography websites.



Figure 1 Avatar Appearance Upgrade

Description: A default Second Life male avatar (left), and the same avatar after upgrading the skin, hair, and eyes (right). Regular users typically upgrade and customize all aspects of their avatars' physical appearance and clothing.

Second Life is characterized by virtual locations (at minimum a room, empty field, or open ocean) populated by characters (avatars) for the users who happen to be at the location. An avatar is an on-screen representation of each person, and may or may not physically resemble the real person (Figure 1). Depending on the restrictions of each particular location, one's appearance can be improved, made to resemble the opposite sex, an animal, or almost anything else. Avatars are able to interact with the environment per the limitations of the software and rules of the location. At minimum one can move around, talk with others (using text and/or voice), and perform tasks related to any number of goals. Users can create as many

avatars as they like. It is possible to change one's appearance in a few seconds and create multiple accounts to prevent identities from being easily connected.

Grasping the Second Life experience requires at least several visits because there is far too much to see and learn in a short period of time. Based on systematic in-world observations, the most visible users are interested in socializing, virtual fashion, music, exploration, role-play, and fantasy experimentation. These activities are supported behind the scenes by computer artists, programmers, 3D designers, and virtual shopkeepers—who may or may not participate in other activities. The in-world user-to-user economy, as used to pay for services and virtual objects, is based on Linden dollars. Linden dollars are exchangeable for real currencies across the world. The majority of users in public locations were observed at sites designed to facilitate chatting, dancing and listening to music, role-playing, shopping, and virtual sex-related activities.

Many Second Life participants appear to be attracted by the freedom of the fantasy world, and the ability to manipulate a wide range of things that generally cannot be altered in real life (e.g., gender, attractiveness, housing, weather, etc.). Some users seemingly return to the era before radio and television when entertainment relied on imagination, live performance, local pubs, and community groups. These activities are best described as a participatory alternative to reading a novel or watching a movie, with each user deciding on the story and how they want their avatar to proceed. Topics range across all those found in traditional art, fiction, and film, such as replicating popular films or TV shows, dancing (Figure 2, page 20), or interacting with original 3D art. In addition, some people indicated that they are disabled or incapacitated and use Second Life to simulate a lifestyle they cannot have in real life, plus there are special interest groups for the disabled.



Figure 2 Avatars at a Dance Club

Description: Avatars looking for dance partners at Sweetheart's Ballroom Dance Club. The gray avatars are in the process of loading.

While crowds of avatars can be found at many virtual clubs and hot spots, other locations are designed to replicate real-world landmarks and tourist destinations (Figure 3 and Figure 4), places of interest to a particular fan group (e.g., a space ship, a gothic vampire castle), or to create objects that would be prohibitively expensive in the real world. Linden Lab publicizes some of the best designed and unique locations in a directory, but they often have few visitors, or people visit one time and then spend hours at socially oriented places. This coincides with the comments of some users that, once they became familiar with and accustomed to Second Life, they keep returning mainly because of their friends. It is also consistent with the general interest in relationship-oriented features across other environments such as social networks and multiplayer games.

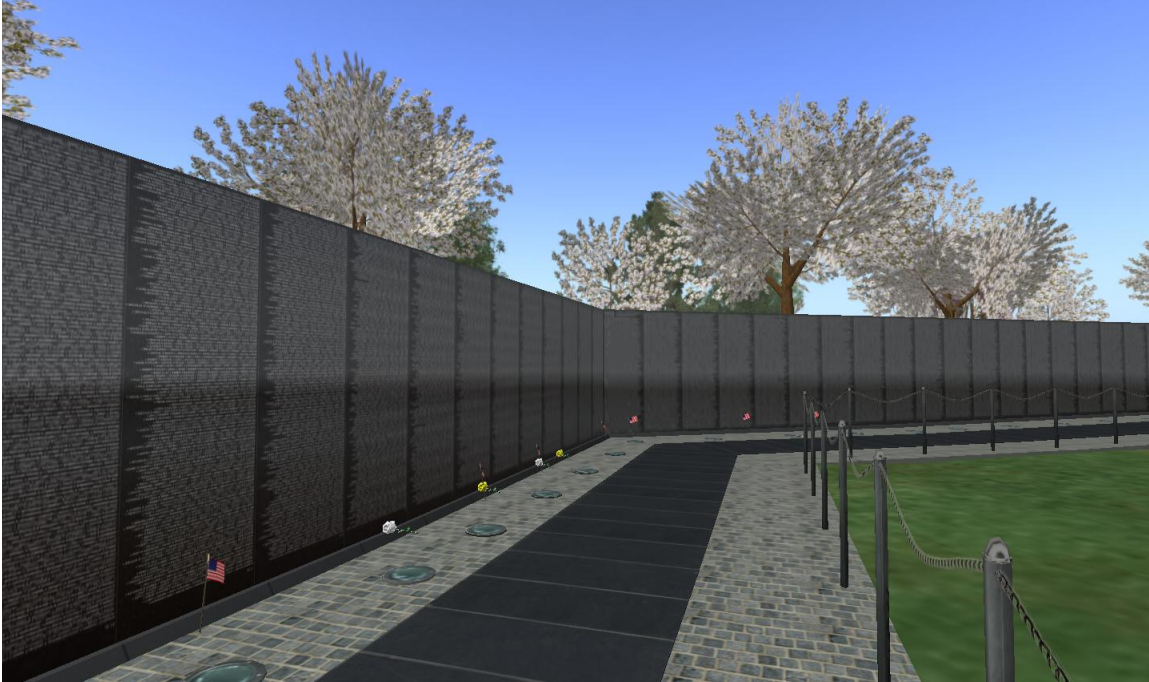


Figure 3 A Second Life version of the Vietnam Veterans Memorial in Washington, D.C.

Readers should not be left with the impression that Second Life and similar products are meant only for entertainment, as graphical content can mislead some into thinking these are just games. Virtual environments have a wide range of educational, business, and professional uses. As mentioned previously, IBM has promoted their use for business meetings (Brodkin, 2008), and the vGov initiative of the National Defense University, U.S. Air Force, Homeland Security Department, and Agriculture Department seeks to develop federal virtual business environments that resemble what can now be done in Second Life (Lipowicz, 2010). Some of the most prominent productivity functions include holding classes or meetings without travel expenses, and allow physical forms of interaction for projects that benefit from visual detail. Examples of such projects include product design and engineering (e.g., collaboration between the diverse range of people working on a new aircraft, ship, or bridge), or architecture (e.g., trying several options for a new office building as seen landscaped and with surrounding buildings).

Summary

Cyber communities such as Second Life duplicate real world activities and forms of interaction in many ways. A wide range of activities are possible, and its users show enduring interest in socializing for shared experiences (e.g., exploration, music, fantasy role-play, etc.). Virtual environments also represent a step forward for business or education productivity goals requiring collaboration, as well as for efficiently completing visually-oriented tasks. In the end, social interaction always occurs between goal-driven people, regardless of the precise details and the surface appearance. It can involve computer text, voice, or video, it can occur over the

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

telephone or face-to-face, and in Second Life, it occurs through graphical illustrations that accompany text or voice conversations.

KNOWN SECURITY ISSUES AND STRATEGIES

This report is a first step toward generating guidance for the personnel security concerns resulting from the emergence of cyberculture. While the primary long-term goal of the project is to address potential new issues and questions requiring additional research, some of the risks associated with social cyber interaction are obvious. In general, those activities that replicate real world behaviors of security concern present little apparent need for deliberation, and may only require updates to policy manuals, employee training, and the allocation of resources for enforcement. However, some differences do require a change in perspective. First, computers increase opportunities for participation in activities of potential interest (e.g., easier interaction with foreign nationals; relationships with limited information about another) so there may be more reportable events from more sources than in the past, and this could magnify the potential for exploitation. Second, the uncertainties inherent with some cyber activities present a range of probably insurmountable limitations to oversight.

False Assumptions of Anonymity and Privacy

The sometimes naïve expectation of online privacy, and the related belief that one can anonymously interact in cyberspace, underlies a wide range of risks. A given user may or may not understand how easily computer software can collect, store, and track behavior, nor understand that many parties do in fact systematically profile Internet users, but all who participate are subject to having private information obtained by others. This occurs through legal, illegal, or unethical means, and despite the intention of being cautious. For example, any online account protected only by passwords and security questions is vulnerable to hacking and social engineering, as occurred with Sarah Palin's private email account during the 2008 presidential campaign. Similarly, at one time hackers obtained databases with the account information of many Second Life users (Kirkpatrick, 2006). Another risk is that friends and associates can post incriminating information on social networks, which is more widely distributed than in the past and stored indefinitely. Finally, a business can enact changes that result in revealing more information than its users intended, as when Facebook decided to share personal data with outside businesses to enable connections between users who visit those websites (Hachman, 2010).

Merely browsing the web exposes one to a wide range of private businesses that collect and aggregate user data from public sources, such as social network accounts, blogs, email, and web browser tracking cookies. A controversy erupted in late 2010 when it was publicized that RapLeaf, Inc. had been collecting real names and detailed user characteristics, which were then transmitted to third-party advertisers. At that time, users were segmented by:

“...household income range, age range, political leaning...gender and age of children in the household, as well as interests in topics including religion, the Bible, gambling, tobacco, adult entertainment and ‘get rich quick’ offers. In all, RapLeaf segmented people into more than 400 categories...”

In response to inquiries, RapLeaf claimed that the sharing of identifying information had been inadvertent, and also eliminated some of the more sensitive categories. Still, during the 2010 election, politicians and political organizations used RapLeaf information to send targeted ads to likely supporters (Steel, 2010). In a similar vein, privacy advocates have sought to raise awareness by compiling public location information from social networks, and then created websites such as PleaseRobMe.com and ICanStalkU.com to highlight how actual people often share information that can easily be exploited (Carton, 2010).

The cleared population faces two major risks due to assumed online anonymity and privacy, including: (1) potential exploitation through databases compiled from public or presumed secure information that track identities, jobs, activities, and associates, and (2) potentially greater willingness to share sensitive information with other people. On the first point, hostile parties can use databases to systematically seek out controlled information and target those most vulnerable to exploitation. As it is impossible to fully control the personal information that appears on the Internet, or the choices of friends, family, and associates to post information, the most practical security strategy is to develop awareness, guidance, and training programs for safe participation. In the examples below and in many other situations, the security implications can be quite different if an activity is linked to one’s real identity. The second point, of how online interaction is associated with disinhibition or depersonalization, is discussed in Part II of the present report. Further research is required to assess whether cleared individuals are in fact more willing to disclose sensitive information, or more accident prone, through cyber interaction than with traditional forms of communication.

Cybersecurity, Cyber Crime, and Counterintelligence

Personnel security measures seek to protect sensitive national security information against loss, compromise, espionage, and other threats, but computer technology has widened the scope of potential risks. For example, a PERSEREC review of changes in espionage points out that the Internet has made it possible for terrorist organizations to form virtual international communities; provides easy access to large libraries of training and political documents; and allows users to employ hacking for communication and to avoid detection (Herbig, 2008). The overall impact of computers has been so significant that Steven Chabinsky, then Deputy Assistant Director of the FBI Cyber Division, called the cyber threat “one of the greatest concerns of the 21st century” (2009).

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

The procedures designed to combat attempts by foreign powers to obtain secure and protected information are described as counterintelligence, but the cyber threat extends well beyond spying and foreign powers. In 2010, Dennis Blair, Director of National Intelligence stated that cybersecurity and counterintelligence efforts were being integrated to improve coverage for the full range of threats. Similarly, the Naval Criminal Investigative Service (NCIS) Cyber Department integrates law enforcement and counterintelligence information (NCIS, 2010). These more generalized responses are required because hostile actions can be functionally identical regardless of an attacker's motivation. For example, one might employ hacking or social engineering to obtain access to a secure computer for personal gain (e.g., theft, blackmail, fraud, and other crimes), commercial gain (e.g., unfair business competition, illegal research and development advantages), or to undermine national security (e.g., obtaining protected information, terrorism, cyber warfare).

Responding to plainly illegal hostile cyber activities often involves a straightforward approach. Specifically, many cyber crimes committed for accessing secured computer systems are merely updates to older confidence (con) games and techniques. Gordon Snow (2010), Assistant Director of the FBI, indicated that some of the most prominent criminal activities associated with social networking websites include social engineering (misrepresentation to gain another's confidence), fraud schemes (simple lies about a product, service, investment, etc.), and phishing scams (attempts to make a user believe information is from a trusted source when it is not). When such crimes occur, the perpetrators are prosecuted through the criminal justice system using the existing standard for a given crime.

The appropriate personnel security strategy for hostile cyber threats is also often straightforward; as cyber interaction largely parallels that of the real world. For example, cyber participants should obviously report any events suggesting attempted espionage, such as abnormal romantic interest on a dating website from a foreign national when the other party might know that one has access to valuable controlled information. Similarly, the current standards used to assess personal responsibility and judgment should be applied to the nuanced negative outcomes of hostile cyber activities. To illustrate, a victim of social engineering might be considered untrustworthy after being persuaded to accept fake money orders from an international party and experiencing severe credit problems as a result.

Foreign Cyber Contacts and Associates

Cyber environments largely duplicate existing personnel security concerns for foreign contacts and associates. Prior to presenting examples of foreign contact in Second Life, the concerns presented in the Adjudicative Guidelines for Foreign Influence, Foreign Preference, and Outside Activities are shown below.

Guideline B - Foreign Influence: Foreign contacts and interests may be a security concern if the individual has divided loyalties or foreign

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

financial interests, may be manipulated or induced to help a foreign person, group, organization, or government in a way that is not in U.S. interests, or is vulnerable to pressure or coercion by any foreign interest. Adjudication under this Guideline can and should consider the identity of the foreign country in which the foreign contact or financial interest is located, including, but not limited to, such considerations as whether the foreign country is known to target United States citizens to obtain protected information and/or is associated with a risk of terrorism.

Guideline C - Foreign Preference: When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

Guideline L - Outside Activities: Involvement in certain types of outside employment or activities is of security concern if it poses a conflict of interest with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

Each of these guidelines is followed by a range of conditions that pertain to contact or association with foreign nationals.

Figure 4 (page 26) shows a group of avatars socializing in a Second Life version of Moscow's Red Square. This is only one of numerous locations in Second Life that reproduce real places across the world. As many users tend to congregate in locations thematically related to their home countries, a user targeting a specific country might log in during peak usage hours for the local time zone (daylight or after work) and visit associated locations (e.g., Red Square for Russia, the Eiffel Tower for France, etc.). Note that locations are typically developed and controlled at the discretion of private owners, so there can be more than one active version of any given real location. At the time this image was captured, several public Russian language text and voice conversations were in progress. Users must share a common language to interact with these apparent Russians or other foreign nationals with ease; however, Second Life has an integrated text translation feature. Additionally, foreign language classes, likely with teachers of uncertain nationality, are conducted in Second Life.

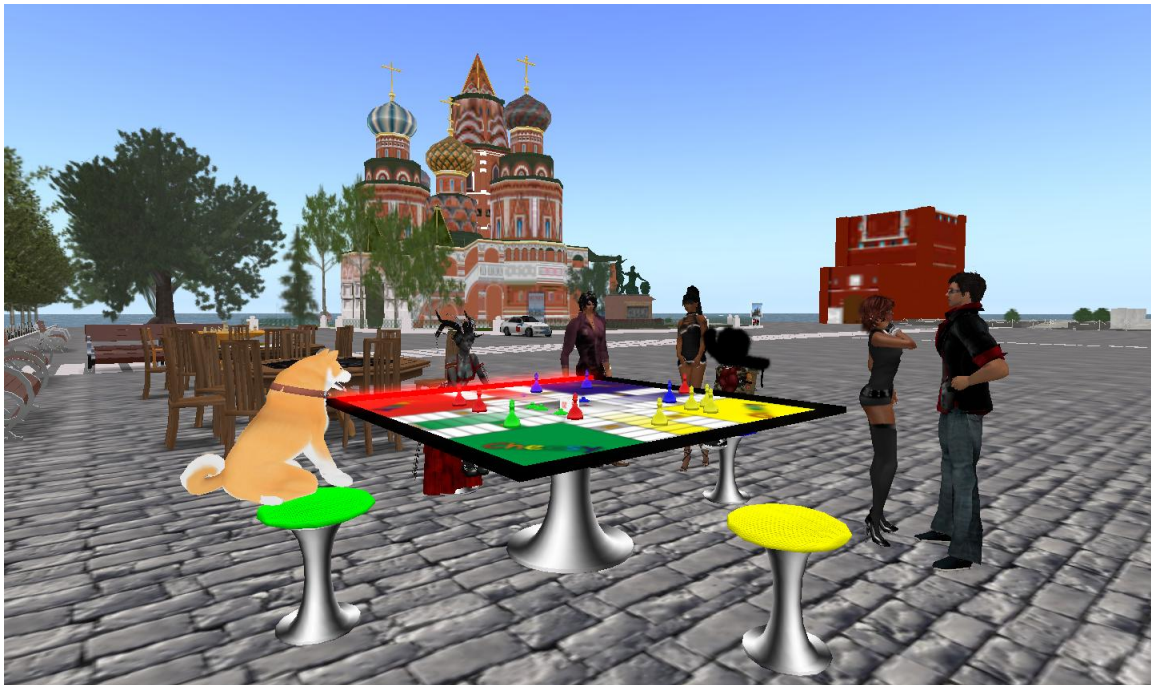


Figure 4 Avatars Playing Games and Conversing in a Version of Moscow's Red Square

Socializing with apparent foreign nationals presents obvious concerns, such as making it much easier to find and target specific countries, but other implicit assumptions do change in this environment. Specifically, (1) each user has full control over their appearance and apparent identity, and (2) barring hacking, the only way to learn another's real identity or personal facts is if the user chooses to share verifiable information, such as a name, email address, phone number, or website. The default status involves deep ambiguity about how to interpret the identity and motives of other users. As also occurs in blogs, text discussion groups, or chat rooms, some purported foreigners may pretend to be foreign to brush up on a rusty language learned in high school, imitate a character from a film, or because they want to see how average people respond to a cultural stereotype (e.g., be "a fish out of water"). Subsequently, the virtual location, a user's appearance, and the language used for communication are not proof of being foreign, and in general the true identity cannot be confirmed. Additional problems can arise among new users who rely on their real world identities, for they may not be aware of the diverse motivations of others and be subject to easy manipulation, extortion, or fraud.

Virtual Government

With the rise of the Internet, many governmental resources and functions are now available online. While any activities undertaken for internal government usage conform to existing security requirements and require access control measures, those involving the general public must occur through open websites and systems. Subsequently, government entry into cyber environments reproduces the personnel security considerations involved with conventional public interaction.

In 2007, the Maldives and Estonia opened official virtual embassies in Second Life (Maldives Mission, 2010; Riley, 2007), both intended for national promotion and to facilitate contact with other countries that do not have physical diplomatic facilities. The Estonian embassy was visited for research. It features a multistoried building with areas dedicated to travel, meetings, and cultural exhibitions. A conference area has facilities for audio-visual presentations. Figure 5 shows the travel visa application kiosk, which provides a link to a conventional website. While international universities and overseas users are extremely common in Second Life, locations intended for official government business appear to be relatively rare. Other examples of content related to diplomacy include a detailed representation of the Swedish Embassy in Washington D.C. that does not provide official services (Simmons, 2007), and a 220-member user group dedicated to assisting real governments to enter virtual worlds.

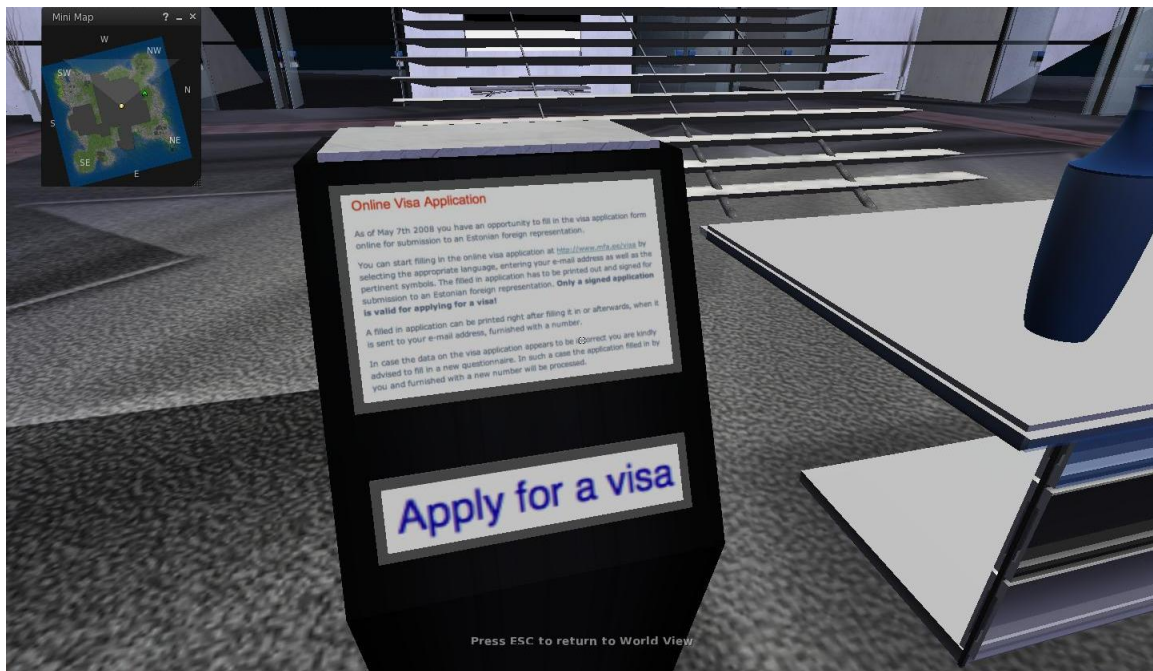


Figure 5 Visa Application Kiosk

Description: The visa application kiosk at the Estonian Embassy in Second Life. The counter to the right is for the Estonian Ministry of Foreign Affairs

Logically, virtual embassies and official government offices could duplicate many security concerns known to affect real embassies, such as facilitating espionage by recruiting visitors as potential intelligence agents. For example, a helpful cyber travel guide might supply a message for delivery to a real world location, turning an innocent tourist into an unwitting and thoroughly unsuspected courier. However, there is no known evidence that such activities actually take place, and the current implementations seem to more closely resemble promotional websites than real embassies. Also, ambiguity cuts both ways, whereby visitors may prove to be unreliable or not useful if real activities are perceived to be part of a game.

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

Conclusions: Cybersecurity Issues

The social activities made possible in cyber environments clearly reproduce existing cybersecurity concerns, and when the identity of another party is known, participation should be subject to the same reporting requirements, investigative attention, and adjudicative review as real world events. If one maintains “close and continuing” contact with a known foreign national or contacts a foreign government through a cyber environment, then it should be reported. Existing questionnaires, investigation, and adjudication documents may require updating to emphasize that cyber environments are subject to current reporting standards, but that do not exceed ordinary requirements for anonymous, isolated, routine, and uneventful physical foreign contact.

Ultimately, the majority of virtual encounters with purported foreigners are probably not worth formal personnel security consideration. This is because there is often no way to confirm the identity of contacts, let alone gain the cooperation of consciously anonymous “foreign” parties who, conversely, could also portray themselves as US citizens to avoid reporting requirements. Other than through self-reports there is no known and practical way for third parties to confirm, evaluate, or monitor cyber participation of many consciously anonymous activities. As foreign governments have little reason to target random individuals, and only minimal information can be gained without a verifiable real world identity, investigation and review of consciously anonymous interaction may often result in dead ends. Future research must assess the costs and benefits of expanded investigation requirements, but in the interim all participants in this sort of cyber environment should receive briefings on the risks and risk mitigation strategies.

Sexual Behavior and Personal Conduct

Personnel security vetting criteria have always considered character and responsibility. For example, when a clearance applicant lies to cover up a minor misdeed, such as a misdemeanor arrest or unpaid debt, it often presents a greater concern for adjudication than the original misdeed. This is because the applicant has consciously violated the terms of employment, has a continuing need to hide the original misdeed, and has created a need to hide the new lie. While many cyber activities duplicate existing personal conduct considerations about lies, character, and covering up issues, the uncertainties of cyber environments limit the conclusions that can be drawn. This is because some activities are not precisely illegal or not precisely lies, for they can be characterized as humor, entertainment, fantasies, or other activities that have no bearing on real world conduct.

The diversity of Second Life, again, provides exceptionally vivid examples of how personnel security concerns for sexual behavior and personal conduct migrate to and are affected by cyber communities. Note, however, that independent sex-oriented virtual environments such as the Utherverses Red Light Center are available, and sexually explicit role-play was once so open and aggressive on a

particular World of Warcraft server that it led to a crackdown by the publisher (Parrish, 2010). For context, the concerns of the Adjudicative Guidelines (2005) for Sexual Behavior and Personal Conduct are reproduced here.

Guideline D - Sexual Behavior: Sexual behavior that involves a criminal offense, indicates a personality or emotional disorder, reflects lack of judgment or discretion, or which may subject the individual to undue influence or coercion, exploitation, or duress can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. No adverse inference concerning the standards in the Guideline may be raised solely on the basis of the sexual orientation of the individual.

Guideline E - Personal Conduct: Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

Second Life allows for customizations that simulate physical world activities. Some of these include dancing, skiing, swimming, and riding in roller coasters or boats. To initiate these activities, the participant selects an object and then the software takes control and begins to animate the avatar, plus the user can often control movements through a menu. Simulated sex between avatars is a now common customization. Virtual sex, or cybersex, involves talking about sex either through typing or voice chat in conjunction with graphically detailed and animated depictions of sex. The simulated acts span those of pornography, extending to nonmainstream and taboo activities such as rape fantasies and bestiality. Other practices include voluntarily entering master and slave relationships, and those soliciting payment as a virtual escort or prostitute who receives Linden dollars for participation in fantasy activities. All of the above activities are legal.

Simulated pedophilia requires special attention because it has led to widespread international concern. At one time, some adult Second Life users changed their appearance to look like children, known as “age play,” and engaged in violent or sexual activities (Terdiman, 2006). This may also provide a loophole for accessing otherwise illegal child pornography, as real photographs of children can be imported into the software and then manipulated to closely resemble actual children. Simulated pedophilia was banned in the United States through the 1996 Child Pornography Prevention Act, but the law was overturned as overly broad in a 2002 Supreme Court ruling. Following this, in 2007 Germany began aggressively tracking and prosecuting simulated pedophilia in Second Life (Francescani & Kucharz, 2007). Linden Lab subsequently enhanced its enforcement of existing

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

policies to eliminate age play, and one of the major age play content providers sought to move to an alternate virtual world (Reuters, 2008).

Personnel security standards for sexual conduct have evolved greatly over several decades, and while not entirely clear, it seems unlikely that they would be applied to simulations between consenting adults meant for private entertainment. It is obviously understood that other forms of sexual entertainment, including pornographic magazines, videos, and websites, phone sex, and interactive video sex are widely available, and in isolation they have no apparent personnel security relevance. Subsequently, the standards for online sex related activities should be similar to established practices. Examples that parallel known concerns include:

- (1) Any sexual content or activity can generate some risk of extortion when the real identities of those involved are known. For example, a 27-year-old man was convicted of trying to blackmail a 14-year-old girl into providing pornographic videos after he obtained explicit photos, and another man in search of explicit photos broke into 3,200 email accounts by resetting user passwords by using information shared on Facebook (McMillan, 2011).
- (2) Ongoing interaction with identifiable people, or when interaction has lead to physical contact, appear to be subject to existing reporting requirements for romantic relationships.
- (3) If virtual and physical prostitution occurs with the same individual, virtual sex activities might be of interest during an investigation to determine the extent of the relationship.
- (4) Simulated pedophilia and simulated child abuse are illegal in some countries, and US law may not yet be settled, so participation presents an apparent risk of international prosecution and blackmail.

Summary

This section presented examples of how current personnel security issues and coverage requirements can directly transfer to cyber activities, and where ambiguities can limit the potential for investigation or adjudicative review. Cyber environments clearly duplicate many real world security concerns, and subsequently should receive systematic and serious consideration. However, these activities should not receive greater attention than real world activities, nor is it worthwhile investigating those lacking relevance or likely to result in dead ends.

Experience has shown that it can be difficult to formulate effective cyber policies, even when it is known that a given activity poses at least some risk. For example, the US Marine Corps briefly banned access to social networks, describing them as "...a proven haven for malicious actors and content and are particularly high risk due to information exposure, user generated content, and targeting by adversaries...." (Marines, 2009), but the ban was lifted a few months later and a new memo instead outlined guidance for responsible, appropriate, and legal use of

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

Internet resources (Marines, 2010). The immediately actionable principles and recommendations derived from Part I of the report are presented below.

- (1) Action should be taken to increase awareness across the personnel security community that cyber activities can be functionally identical to real world activities and can present similar risks. Cyber activities that are reportable per the current Adjudicative Guidelines should be explicitly considered along with real world activities. The examples suggest several requirements and strategies for further consideration:
 - (a) Cyber relationships with foreign nationals or virtual romantic partners, when the real world identity of a cleared individual is shared, might be investigated and adjudicated per the existing standards for these topics.
 - (b) Any experience of hostile cyber threats (i.e., from foreign parties, extortionists, or others who know a user's real world identity) should be reported and investigated on an equal footing with real world reporting of such activities.
 - (c) Participation in simulated child pornography or simulated child abuse may be reportable because of international laws and the associated potential for blackmail.
 - (d) It is unlikely that reviewing intentionally anonymous contact with purported foreigners, fantasy romantic partners, or others will be possible, productive, or cost effective. This is because people can continuously create multiple new anonymous identities, there is no known way to determine the identities of other anonymous parties without affecting general privacy rights, and most actions have no apparent personnel security relevance.
- (2) All established cybersecurity topics, such as cyber money laundering, hacking, gang activity, and organized crime, should be systematically reviewed to update personnel security reporting and evaluation guidance.
- (3) No policy, reporting, or enforcement changes should be made to address novel cyber activities that do not derive directly from existing real-world personnel security standards, unless the changes are supported by empirical evidence.
- (4) As outlined in Part II of the present report, personnel security policymakers should address how best to evaluate and manage participation in cyber environments. The core needs are to:
 - (a) Define new and unique cyber topics of potential personnel security interest. Part II presents a range of topics for consideration, and is meant to guide research for this need.
 - (b) Determine the costs and benefits associated with covering new topics.

PART I: ORIENTATION AND ACTIONABLE STRATEGIES

- (i) Assess potential for collecting and validating data, considering anonymous participation, the dark web (private, unsearchable content), hijacked content (content copied, stolen, or taken out of context), content stored internationally, and respect for the privacy and civil rights of the general population.
- (ii) Generate self reporting requirements and clearly specify investigative boundaries.

Part I provided an overview of cyberculture in the general cybersecurity context, outlined important considerations and unanswered questions for personnel security, provided detailed examples of how cyber activities can duplicate known real world issues, and listed immediately actionable recommendations. Part II sketches the state of research knowledge to look to the future and how move forward in responding to the threats posed by cyberculture with greater precision and more comprehensively.

PART II: SCIENTIFIC CONTEXT AND RESEARCH GUIDANCE

CYBERCULTURE AND PSYCHOLOGY

This section presents examples of the logic and research evidence for how cyber activities might result in personnel security, psychological, and workplace concerns—and therefore helps guide future research. Society is in the process of learning how rapidly evolving technologies such as personal computers, cell phones, mobile electronics, and wireless network access affect culture, how they solve old problems, and how they create new concerns. Research to understand the impact of these technologies can only occur as products become available and popular. There are no known data on the psychological impact of cyberculture among potential security clearance applicants or current holders, so targeted research is required. The most prominent concerns for personnel security appear to fall into two broad categories: (1) how the ability to manipulate personal information and control virtual relationships may affect standards for real-life loyalty, reliability, and trustworthiness, and (2) how constant availability may enable or promote impulse control disorders and addiction. The examples below highlight the need for focused research on cyberculture, psychology, and personnel security, but should not be regarded as an exhaustive list of all topics of potential concern².

Computer Mediated Relationships and Disinhibition

A common observation is that people interact differently in cyberspace than offline, such as being more willing to disclose private information about the self, express secret emotions, engage in virtual sexual intimacy, express harsh criticism of strangers, willfully disrupt discussions, etc. For example, research has shown that frequent online chatters are more likely to disclose intimate and personal details than nonfrequent chatters (Leung, 2002). McKenna and Bargh (2000) describe this effect as deindividuation, and Riva (2002) cites work indicating that the absence of face-to-face cues leads to argumentative and destructive interactions, while Suler (2004) calls this phenomenon the *online disinhibition effect*. Furthermore, Suler's detailed analysis separates *benign* disinhibition, including reduced fear, shyness, and greater generosity, from *toxic* activities such as rudeness, anger, hatred, and accessing violent or pornographic material.

Disinhibition is a useful concept for summarizing how interpersonal interaction often changes in cyberspace. Making social contact and forming or maintaining relationships from behind a computer display facilitates things that are not possible or practical in the real world. There is no eye contact, body language, or other

² The present research is concerned with personnel security, as general information on cyberculture is available from numerous other sources. For example, Barak (2010) maintains a website dedicated to cataloging research on psychology and the internet conducted since 1996. It includes sections on research about children, the elderly, addiction and crime, gaming and gambling, virtual communities, and many other topics.

PART II: SCIENTIFIC CONTEXT AND RESEARCH GUIDANCE

behavioral evidence of a person's mood and attitude. It becomes easy to present oneself as an expert, impersonate a public figure, and lie about location, job, gender, or age. People can express taboo or bigoted thoughts, and say things that would offend friends and family. Furthermore, a person need not respond to others immediately, and so can more precisely calculate and construct answers. McKenna and Bargh (2000) reviewed research comparing virtual versus face-to-face interaction and summarized differences that remain central today. They concluded that computers permit: (1) being anonymous, (2) developing relationships regardless of physical distance, (3) forming relationships without consideration of physical appearance, and (4) interacting without regard for an immediate response, such as through email and text messaging. Several examples of how these changes interact with potential security risks are presented below.

Openness and Risk Taking

McKenna and Bargh (2000) discuss how the Internet creates a safe zone and blank slate for fantasy experimentation. One can create many alternate versions of the self, with the possibility of exploring fringe politics, homosexuality, and other activities that may lead to stigmatization among certain cultural groups. Their prior empirical studies found that, when online, people tend to present idealized selves and favor strangers better than when meeting the same person face to face. However, they also note that a fantasy self might potentially lead to delusional or unrealistic real-world behavior; and as anonymous conversations lack the consequences of real life activities, they often create a false sense of interaction (Shapira, et al., 2003). From a personnel security standpoint, if a great deal or the majority of communication is unconstrained by the repercussions of personal disclosure, there is a possibility that this may lead to forming relationships abnormally fast and expressing thoughts without restraint. In turn, this could ultimately lead to the unintentional disclosure of sensitive or classified information.

From an ordinary cultural and psychological standpoint, meeting new people, exploring unfamiliar cultures, and trying new experiences are generally perceived as having positive consequences. In contrast, personnel security background screening criteria require the reporting of, and therefore potentially discourage, foreign contact and association. For example, Suler's (2004) analysis of online disinhibition describes the increased willingness to disclose personal information as a "benign" effect, yet accidental disclosure (e.g., during absentminded conversations) is a significant concern with sensitive or classified information. This is compounded by the fact that cyber communities allow people to easily form relationships across national borders, with no vetting of the foreign nationals or even the possibility of determining their true identities. Similarly, if individuals engage in fantasy taboo activities and fear being discovered, they might go to great lengths to hide their interests and associations from a spouse, coworker, or employer. A Time Magazine story described how a real-life marriage that began with a meeting in an online chat room later ended amid accusations of Second Life

affairs, the hiring of virtual private investigators, attempts at virtual seduction, and claims of cyber addiction (Adams, 2008). As discussed above, the potential for blackmail in cyberculture is similar to that in the conventional world, and should be consistently considered during background investigations.

Targeted personnel security research must assess how so-called “benign” disinhibition bears on unintentional disclosure of sensitive or classified information, Foreign Influence and Preference concerns, and other disqualifying behaviors from the Adjudicative Guidelines. The systematic observations of Second Life provided widespread evidence of disinhibition. Consistent with the notion of unrealistic interaction, most Second Life avatars have idealized bodies (e.g., extremely tall, fashionable, long legs, complex hairstyles) and are often hyper-masculine or hyper-feminine. “Friendships” are formed quickly and easily, but often end without notice when the one party simply deletes the other party’s contact information. With regard to blackmail, some avatars informed the research staff that they were “deep undercover” when asked if friends and family knew about their involvement, introducing the risk of blackmail or exploitation. The Second Life ethnography described in Report II addresses these concerns and findings in detail.

Misrepresentation and Deception

The honesty of clearance holders is a core consideration for personnel security, as accurate information is essential for conducting a background investigation and the basis for trusting an individual with sensitive information. In contrast to how society functioned decades ago, the relative anonymity and confidentiality available online offers great opportunities for exaggeration or outright deception with regard to one’s true identity and competence (Suler, 2004). People are also widely aware that cyber environments increase the potential for misleading others and believe that online deception is extremely common (Caspi & Gorsky, 2006). However, while opportunities for deception are clearly present online, the reviewed research indicates that in practice: (1) deception is not necessarily more common online than offline, (2) people tend to present themselves in an idealized but largely realistic light, but (3) deception occurs most often in anonymous communities and where there is limited potential for verifying facts or affecting everyday life (Zhao, Grasmuck, & Martin, 2008; Caspi & Gorsky, 2006). From a personnel security standpoint, it is important to understand why and when deception does occur, and how misrepresentation varies by context. The reasons are presented below.

Cyber communities that focus on the real world are rooted in conventional standards for disclosure and honesty. When a person seeks a continuing and real relationship, deception is counterproductive because it will undermine trust if discovered. The core goals of dating websites and social networks are largely incompatible with outright lies, so the distortion in these communities tends to be used to put oneself in the best light, such as being friendly, popular, successful, well-rounded, and having good taste (Zhao, et al., 2008). This is consistent with research indicating that increased use of Facebook is correlated with narcissism

PART II: SCIENTIFIC CONTEXT AND RESEARCH GUIDANCE

and low self-esteem (Mehdizadeh, 2010). However, social networks facilitate another sort of misrepresentation through the reportedly common practice of creating multiple personas and false identities (Riva, 2002; Subrahmanyam & Greenfield, 2008; Boutin, 2010). These can be used to separate information available to particular circles of associates (e.g., friends vs. family vs. workplace) and shape the impression given to contacts. It is not clear whether this practice constitutes a form of misrepresentation important for personnel security vetting, but there may be a legitimate need to know if employees are leading double lives.

Cyber communities with optional anonymity (e.g., Second Life, games, and blogs) allow the greatest potential for misrepresentation. For example, claims of having homosexual or nonmainstream sexual preferences have been found to be less common on Facebook than in chat rooms and anonymous environments (Zhao, et al., 2008). There is often no practical way to determine whether such individuals are truly interested in participation, or if they have an ulterior motive such as trying to stimulate discussion or generate a reaction. Conventional ethical standards appear to change the most when there is anonymity and few consequences for deception, such as with some multiplayer games. In the online word game Lexulous (similar to Scrabble) users frequently misrepresent their competence by using external scrabble solver engines that unscramble letters and display possible words during competitive games. Although this practice would be considered cheating in a real-world tournament, it is not considered unethical by the users in this context (Slatalla, 2009).

Returning to the project goal of understanding how cyberculture may affect personnel security interests in character, reliability, and judgment, questions requiring future research include: (1) whether general cultural standards for honesty might be affected by extensive, long-term interaction among those who do not value honesty, such that dishonesty adversely affects the workplace, and (2) whether some individuals might become confused about what constitutes appropriate workplace vs. cyber behavior. The reviewed publications suggest that most people tend to adopt similar standards and approaches both online and offline (Caspi & Gorsky, 2006; Subrahmanyam & Greenfield, 2008; Zhao, et al., 2008), but there are hints that cyber participation may be associated with measurable changes in ethics or morality. For example, a survey found that frequent participants in discussion groups lied more often than infrequent participants; and in contrast with real life lies, online lies were primarily seen as enjoyable and not associated with negative emotions (Caspi & Gorsky, 2006). It is also not clear whether and how particularly malicious individuals might use cyber environments for gain over those users who maintain their real world personas.

Hostility and Aggression

Participants in cyber communities have long known that some people become much more hostile, aggressive, and blunt online than they would be in real life. In discussion groups, unchecked criticism or anger is known as “flaming,” and

mentioning controversial topics to stir up a response is known as “trolling.” These are examples of toxic online disinhibition per Suler’s (2004) analysis, and they occur in a wide range of communities, including user comments about news stories, political discussions, special-interest blogs, social networks, games, and chat rooms. The associated personnel security concerns are that cyberculture might lead to an increase in real-world aggression, or that cultural acceptance of overt hostility could affect workplace management.

Cyberbullying involves using electronic devices for intentional and repeated aggression against those who cannot mount an effective defense (Smith, Mahdavi, Carvalho, & Tippett, 2006). It has received extensive legal and media attention in conjunction with suicides. For example, Lori Drew, the mother of a former friend of 13-year-old Megan Meier, created a false social network profile and befriended the girl, but then later turned on her in revenge for perceived mistreatment of her child, which drove Megan to take her own life (Collins, 2008). Following Megan’s suicide, Lori Drew was tried and convicted of three misdemeanors, but the case was eventually dismissed by the judge (Zavis, 2009). Similarly, five Massachusetts students were criminally charged for systematic bullying (both cyber and conventional) associated with the suicide of Phoebe Prince, a 15-year-old ninth-grader from Ireland (Bazelon, 2010). Surveys of urban Canadian adolescents by Li (2006, 2007) indicate that about a quarter of junior high students have been victims of cyberbullying, and almost 15% have themselves been cyberbullies (12% of females, 22% of males).

While the motives for bullying are similar in any situation, computer technology makes it easier to attack anonymously, take embarrassing pictures, create critical websites, store information that cannot be removed, and widely distribute hostile messages. The next generation of security clearance holders will have lived through such experiences, and events that might have once been “skeletons in the closet” could become widely known and permanently available. Li (2007) notes that many adolescents are naïve about appropriate safety strategies for cyberspace, and often do not report bullying to adults. Subsequently, background investigations may soon uncover new types and a greater volume of potentially derogatory information, and being a bully or being bullied may have longer lasting effects. Research is necessary to determine the implications and formulate an appropriate response.

Another concern involves participation in violent video games, which have been widely researched for potentially increasing real-world aggression and negatively impacting school performance (Gentile, Lynch, Linder, & Walsh, 2004; Ivory & Kalyanaraman, 2007; Konijn, Bijvank, & Bushman, 2007). For example, Konijn et al. had adolescent boys with low educational ability play violent or nonviolent video games and then later asked them to “play sounds for a partner” when they were told that the volume could be loud enough to permanently damage the partner’s hearing. Those who played violent games and wishfully identified with aggressive, remorseless game characters were more likely to play damaging sounds even when not provoked. This seems to be of particular interest to the military, where

PART II: SCIENTIFIC CONTEXT AND RESEARCH GUIDANCE

unjustified violence against civilians during combat can lead to increased resistance and undermine the chances for a successful campaign. For example, in late 2003 U.S. military personnel abused and tortured prisoners at Abu Ghraib in Iraq, and also took graphic photographs of their actions (Hersh, 2004). As a potentially contributing factor, the role of violent video games should be evaluated.

Impulse Control and Cyber Addiction

Cyberculture facilitates a wide range of activities and forms of social interaction that can be difficult to find or organize in the real world. These are often done in private and without feedback from friends or family, and relationships can exist purely through computers. If desired, a person can use computers for remote employment, shopping, socializing, and entertainment. A concern in the scientific and popular press is that computer-related technologies can lead to cyber addiction. Cyber addiction is a behavioral addiction that entails excessive use of specific cyber environments or cyber space in general, resulting in negative psychosocial and professional impairments to a person's life, to include personal, school, and work difficulties (Caplan, 2002; Caplan, Williams, & Yee, 2009; Beard & Wolf, 2001; Shapira, Goldsmith, Keck, Khosla, & McElroy, 2000). The notion of cyber addiction is relatively new, but it has received a great deal of attention in the scientific literature. Other terms for this phenomenon include compulsive computer use or pathological Internet use, and share common features with impulse control, substance abuse, and obsessive-compulsive disorders from DSM-IV. An influential editorial written by Jerald Block in the *American Journal of Psychiatry* in 2008, made a case for why cyber addiction should be included in the *Diagnostic and Statistical Manual of Mental Disorders*, 5th Ed. He argued that because the symptoms involve excessive use, withdrawal, tolerance, and negative repercussions, it should be added to the spectrum of recognized impulse control disorders.

Poor impulse control, or taking action without consideration of the longer-term consequences, appears to be associated with a wide range of potentially disqualifying behaviors in the Adjudicative Guidelines, including psychological conditions, criminal activity, financial mismanagement, drunk driving, and more. In all manifestations, with or without addiction per se, this deficit can undermine individuals' reliability, judgment, and trustworthiness to handle and safeguard classified information. Importantly, however, certain individuals may exhibit problems in some contexts (such as online games) but not others (such as finances), so a broader range of activities may require consideration during investigations and adjudication. For example, a Subject might honestly not report any psychological, criminal, or financial problems per the current Standard Form 86 (SF-86) questions during a background investigation, but still play games during work breaks, evenings, and weekends for upwards of 30-40 hours per week. This could impact alertness on the job and create direct risks when operating complex equipment, driving vehicles, or using weapons. In 2008 a commuter train engineer sent a text message 22 seconds before a crash that killed 24 people and caused

\$10.6 million in damages. He had previously been caught twice on the job with a cell phone (CNN, 2009).

A large-scale epidemiological study of problematic cyber use (Aboujaoude, Koran, Gamel, Large, & Serpe, 2006) found that between 3.7% to 13.7% of U.S. adult Internet users met one or more diagnostic criteria for impulse control disorders, such as feeling that personal relationships have suffered as a result of excessive cyber use, feeling preoccupied by the Internet when offline, finding it difficult to stay away from the Internet for several days at a time, etc. Some have outlined theoretical frameworks and implications for cyber addiction. Block (2008) characterizes cyber addiction as involving online and/or offline computer usage, and consisting of at least three subtypes: excessive gaming, preoccupations with online sexual behavior, and email/text messaging. The three subtypes of cyber addiction all share the following characteristics common to addictive disorders: (1) excessive use, associated with a loss of sense of time or a neglect of basic biological drives, (2) withdrawal, accompanied by feelings of anger, tension, and depression when the computer is inaccessible, (3) tolerance, including the need for better computer equipment, more software, and more hours of use, and (4) negative repercussions, including disagreements, lying, poor achievement, social isolation, and fatigue.

Online multiplayer games clearly illustrate the potential impact of heavy or addictive computer use. Hardcore gamers have been known to play all night long, skip meals, fail to exercise, and have even died during extended play sessions (Anderson, 2001; Nalwa & Anand, 2003; Young, 1998; BBC News, 2005). Users of massively multiplayer online role-playing games (MMORPGs) such as World of Warcraft and Everquest often play in a fashion that many consider to be excessive. Research indicates that the design of World of Warcraft is consistent with behavioral conditioning principles for encouraging more play and longer play—as one goal of the developer is to prolong player subscriptions and increase profits (Ducheneaut, et al., 2006). A survey of 7,000 EverQuest 2 players found that an average player is 31.16 years old and plays an average of 26.86 hours a week (Williams, Yee, & Caplan, 2008). Ng and Wiemer-Hastings (2005) reported that 34% of surveyed MMORPG users played for 21-40 hours per week and 11% played for more than 40 hours per week, but only 4% and 2% of non-MMORPG players fell into the same hourly categories. Finally, Yee (2004) reports that 50% of MMORPG players consider themselves addicted.

Summary

This section presented examples of why personnel security needs to consider the impact of cyberculture on employees' fitness to handle classified information and occupy sensitive positions. However, these examples must not be viewed as the final word or specific recommendations, because necessary data are not yet available. A long history of research in personality and social psychology indicates that the impact of any medium varies between individuals and situations, and is

PART II: SCIENTIFIC CONTEXT AND RESEARCH GUIDANCE

shaped by goals and motivations (McKenna & Bargh, 2000). Subsequently, as with all other behaviors, cyber participation must be examined using the whole person concept and with appropriate consideration of mitigating factors.

Empirical research must assess if and how cyber involvement can result in demonstrable negative real world consequences. For example, reliance on anonymous relationships or adopting potentially reckless and unethical norms may result in inappropriate workplace behavior. Having a pattern of weak one-sided relationships may lead to unrealistic expectations for control and a desire to avoid unpleasant situations or responsibility. The adoption of cyber world norms may translate into workplace behaviors of security concern, such as being secretive, breaking rules, and lying. Finally, cyber addiction poses a likely security risk because of close parallels to impulse control disorders known to affect judgment, reliability, and trustworthiness, such as gambling and alcoholism.

CYBERCULTURE AND MALADAPTIVE SPILLOVER

A core goal of this project is to determine if and how maladaptive involvement in cyberculture might have significant negative consequences for the personal and professional lives of clearance holders that could impact personnel security. While the section above described how cyberculture can affect cognitive outcomes, this section reviews findings on the relationship between cyber use and mental and physical health outcomes, as well as employee behavior in the workplace. Good mental and physical health is important because both are conditions of employment for many sensitive positions (e.g., Department of Defense Personnel Reliability Program [PRP] positions requiring employees to work with nuclear weapons; Department of Defense, 2006). Workplace behavior must be considered to assess whether cyber behavior might negatively affect judgment, as poor judgment in the workplace can be a serious security risk requiring prompt attention. It is presently unclear whether cyber involvement occurring outside work significantly affects workplace behavior, so this question requires exploration.

Mental Health Outcomes

Scientific research examining the impact of cyber involvement on mental health outcomes can be divided into two categories. Type I studies characterize cyber use by the average number of hours per week spent in cyberspace. These studies select participants through questionnaires on their cyber involvement and various indications of mental health functioning (e.g., mood, self-esteem, etc.). During the data analytic phase, the time spent in cyber space is correlated with evaluations of mental health functioning, and/or statistical modeling techniques are used to understand whether the time spent in cyber space and demographic characteristics predict mental health functioning. Type II studies define cyber use as the presence of clinical symptoms descriptive of compulsive-impulsive spectrum disorders from the DSM-IV. These studies typically examine individuals with diagnosed cyber addiction problems, detected either upon seeking counseling or through those who

happen to have extreme scores on measures of cyber addiction. Participants in Type II studies fill out questionnaires about their cyber involvement or participate in detailed interviews on the experience of cyber addiction. Results from Type II studies can only be generalized to individuals suffering from diagnosed cyber addiction.

The findings of Type I studies are most relevant for estimating and understanding spillover in the population of clearance holders, whereas the findings from Type II studies will have limited applicability for most functional employees. This is because only a fraction of individuals experience clinical symptoms of cyber addiction (Aboujaoude et al., 2006). However, the clinical cases presented in Type II studies are helpful for illustrating cyber addiction in detail and the potential risks facing the cleared workforce.

The consensus findings of Type I studies are that the amount of time spent in cyberspace is correlated with diminished impulse control, depressed mood, loneliness, reduced social support, low self-esteem, and withdrawal from family activities (e.g., Armstrong, Phillips, & Saling, 2000; Caplan, 2002; Davis, Flett, & Besser, 2002; Kraut et al., 1998; Meerkerk, 2007). In other words, the more time individuals spend in cyberspace, the more likely they are to report experiencing these negative mental health outcomes. Nearly all of these Type I studies did not differentiate between specific and generalized cyber use (Davis, 2001). “Specific” cyber use refers to the amount of time spent using a given cyber environment (e.g., Facebook, World of Warcraft, or Second Life), whereas generalized use refers to the overall amount of time spent in cyberspace. It is likely that some of the negative mental health effects observed in Type I studies pertain to particular types of cyber environments (e.g., the massively multiplayer online role-playing game EverQuest 2; Ng & Wiemer-Hastings, 2005). Future research should systematically distinguish between specific and generalized cyber use.

The findings of Type II studies suggest that, compared to normal people, cyber addicts are more likely to experience mood and anxiety disorders such as depression and bipolar disorder, substance use disorders, personality disorders, emotional distress, loneliness, family problems, and withdrawal symptoms when their cyber access is taken away (Black, Belsare, & Schlosser, 1999; Chappell, Eatough, Davies, & Griffiths, 2006; Morahan-Martin & Schumacker, 2000; Shapira et al., 2000; Young & Rogers, 1998). To illustrate, Shapira et al. (2000) interviewed people who experienced problematic cyber use and spent more than 30 hours a week in cyberspace for the past 3 years. In addition to suffering from a number of psychosocial impairments, all of the participants met the diagnostic criteria of an impulse control disorder not otherwise specified, and nearly all met the criteria for manic depression or a psychotic disorder with similar features while the others had a history of anxiety disorders, substance abuse problems, impulse control disorders and eating disorders.

PART II: SCIENTIFIC CONTEXT AND RESEARCH GUIDANCE

In aggregation, the findings of Type II studies suggest that cyber addicts suffer from a great deal of psychological distress, which may not only affect their day-to-day well-being, but also their judgment in the workplace. Converging evidence for the diminished ability to make decisions comes from a study by Immordino-Yang, McColl, Damasio, & Damasio (2009). These scientists showed that rapid exchanges of information from text messaging and microblogging (e.g., Twitter, Tumblr) websites could actually harm individuals' moral and emotional development, by not allowing users to sufficiently process information before responding. Ironically, individuals may be turning to various cyber environments to reduce psychological distress, but in doing so they withdraw from real-life social contact and only exacerbate it further (Davis, Flett, & Besser, 2002; Kim, LaRose, & Peng, 2009).

Physical Health Outcomes

Little empirical research on the associations between cyber use and physical health has been conducted; however, theoretical work published in the *Biologist* shows that excessive cyber use can harm health by reducing the amount of face-to-face contact among individuals (Sigman, 2009). Additionally, several studies have examined the relationship between cyber use and sleep (Anderson, 2001; Nalwa & Anand, 2003; Young, 1998). Finally, various media accounts suggest that in extreme cases, excessive cyber use can result in death.

In his *Biologist* article, Sigman (2009) discussed the biological implications for public health of social networking and communicating through computer-based technologies. He argued that increased reliance on computer-based communication should be considered a growing public health issue, with negative implications for eye and ear contact, gene expression, sleep efficiency, immunological changes, morbidity, and mortality. Sigman's overarching hypothesis is that by communicating with others virtually we become socially isolated from our physical networks of friends and family, which in turn makes us more vulnerable to various adverse health outcomes. Although the direct relationship between cyber communication and physical health has not been investigated longitudinally, there are well-established links between cyber use and loneliness (e.g., Kraut et al., 1998, Leung, 2002) and between loneliness and markers of health and well-being (e.g., Cohen, Doyle, Skoner, Rabin, & Gwaltney, 1997; Hawkley, Thisted, & Cacioppo, 2009; Lund, Christensen, Holstein, Due, & Osler, 2006), thereby lending credibility to Sigman's hypothesis that cyber use could harm health.

Excessive cyber use has been found to lead to the loss of sleep. In several studies comparing cyber addicts with normal controls (Anderson, 2001; Nalwa & Anand, 2003; Young, 1998), cyber addicts reported frequently losing sleep due to late night log-ins. Addicted participants would stay online until early morning hours, despite knowing they had to be at work or school early the following morning, or knowing they would feel fatigued the next day. In extreme cases, participants even reported using caffeine pills to continue their cyber use. A large number of individuals also indicated that they stopped exercising or attending to personal hygiene, and often

skipped meals because of cyber use. For the present project, the research staff read several hundred stories of addiction posted by users and their family members on the On-line Gamers Anonymous (OLGA) website (www.olganon.org). The postings resonated with the published findings, through comments about suffering from a loss of sleep, lack of proper nutrition, and lack of exercise.

Finally, a number of media accounts suggest that, in extreme cases, cyber overuse can have fatal consequences. In 2008, a 15-year-old boy in Sweden collapsed and went into epileptic convulsions after playing World of Warcraft for more than 24 hours straight. Medical authorities ruled that the epileptic seizure was caused by sleep deprivation and lack of food, as well as staring at a screen and concentrating for hours on end (Fox News, 2008). A 28-year old man in South Korea died after reportedly playing an online computer game for 50 hours (BBC News, 2005), and the police reported the cause of death was heart failure stemming from exhaustion. The young man had also not been sleeping properly or eating well for a long period of time, and had been recently fired because of constantly missing work to play the game. A similar fatal case in China involved a 27-year-old man who died at an Internet café after playing a game for 32 hours (VNUnet News, 2002). Suicides have also resulted, as with a 13-year-old boy who died while trying to recreate a scene from the World of Warcraft (Fox News, 2006). His suicide note stated that he jumped from a tall building to reunite with the heroes of the game he worshipped. Another suicide occurred in Wisconsin, where a 21-year-old EverQuest addict fatally shot himself in front of his computer after being rejected by another player (Fox News, 2007). Finally, there have been several cases involving small children dying from neglect because their parents were addicted to playing online games (MSNBC News, 2007).

Workplace Outcomes

There are several ways that cyber involvement might spill over to the workplace and create personnel security risks. First and foremost, relaxed attitudes and habits for lying and rule breaking that are generally accepted in cyberspace could become more problematic in professional contexts. Second, individuals may work less than scheduled or required because of compulsions to access blocked cyber environments, or attempt to access blocked environments at work by bypassing information security barriers (Greenfield & Davis, 2002; Shapira et al., 2000; Young, 1998). This concern applies primarily to organizations that both block employee access to the relevant websites and do not permit external wireless devices at work. In contrast, those organizations that permit electronic devices face the problem of employees accessing websites through personal devices without leaving any traceable evidence. This activity subjects employees both to the potential psychological spillover resulting from addiction and the risk of inadvertent disclosure of sensitive work information.

A large number of studies have shown that cyber addiction is linked to several negative outcomes occurring both at home and in the workplace (Greenfield &

PART II: SCIENTIFIC CONTEXT AND RESEARCH GUIDANCE

Davis, 2002; Kraut et al., 1998; Morahan-Martin & Schumacher, 2000; Padilla-Walker, Nelson, Carroll, & Jensen, 2009; Young & Rogers, 1998). A national household telephone survey conducted by Aboujaoude et al. (2006) concluded that cyber use has become a consuming societal problem. Moreover, cyber addiction may be a risk factor for other behavioral and substance-related addictions that impact the workplace, such as pathological gambling and alcoholism (Black et al., 1999).

Finally, cyberspace is characterized by easy access, affordability and anonymity (King, 1999), and is, therefore, effective for concealing pornographic activities from coworkers (Cavaglion, 2008; Young, 2008). Online sexual preoccupation can affect the workplace when employees access pornography at work. It was revealed that more than 30 DoD employees with high-level security clearances, employed at organizations including the National Security Agency (NSA), National Reconnaissance Office (NRO), and Defense Advanced Projects Research Agency (DARPA), have been investigated since 2002 for the possession of child pornography. Some accessed this material from government computers, and one individual had stored 93 documents, 8,400 pictures, and 200 movies (Bender, 2010). Online sexual preoccupation is risky from a personnel security standpoint for several reasons. First, it entails significant financial consequences for employers due to the loss of labor and productivity. Second, it may result in blackmail of the employee. Third, the apparent lack of impulse control on the part of an employee signals impaired judgment and poor decisionmaking ability, which could translate into difficulties in following rules or adequately protecting classified information. Finally, online communication about sex at work introduces the risks of inadvertently revealing sensitive information or being pressured to reveal sensitive information during these interactions.

Summary

This section has reviewed a wide range of evidence and research findings for how cyber participation may be associated with serious negative mental health, physical health, and workplace outcomes. Spillover effects related to reliability, trustworthiness, and judgment can be of great concern for many sensitive personnel security positions. For mental health, research suggests excessive cyber use may be associated with impulse control problems and depression, but more specific research is required. For physical health, excessive cyber use has been associated with loss of sleep, lack of exercise, poor nutrition, and even death. For the workplace, excessive use could lead to increased acceptance of rule breaking, with potential consequences for the security measures designed to protect controlled information, the loss of productivity, and potential exposure to legal liabilities. Future research needs to address the overall impact of spillover and provide actionable recommendations.

GENERAL DISCUSSION

This report has outlined the changes facing society with the emergence of cybercultures; described the purposes and capabilities of several cyber environments; presented detailed examples from the virtual social environment, Second Life; highlighted why cyber behaviors can be of personnel security concern; and reviewed scientific literature on the psychological and potentially adverse real world impact of participation. Cyber environments are playing an ever larger role in modern life, seemingly because they provide so many benefits for socialization, business, shopping, entertainment, and education. However, they also expand the range of potential personnel security risks. Some risks, such as facilitating contact with foreign nationals, largely duplicate established issues and are presently reportable. Other topics requiring research include impulse control problems or addiction, physical and health problems, and potential changes in socialization that are inconsistent with present standards for telling the truth and privacy. Data pertaining to many central personnel security questions are not yet available, so research must be conducted to generate actionable guidance.

Next Steps for the Cyberculture Research Program

Empirical research is necessary to better understand the psychological, workplace, and real life impact of cyberculture participation, as affecting personnel security. This research is in its early stages and faces several major questions. First, there are no known data on how frequently clearance holders participate in cyber communities and what behaviors they choose. Second, there are few data showing whether participation has any measurable impact on outcomes of concern to personnel security, such as judgment, reliability, and trustworthiness. Third, it is possible that any effects will change, moderate, or broaden over time as cyber communities grow and the participants settle into long-term usage patterns.

Given the above considerations, this project was planned as a multi-phase investigation to evaluate the personnel security impact and identify best practices for handling new issues that are presently unaddressed by the vetting process. The first empirical step, as presented independently in Report I, was to gather basic information on activities that are potentially relevant to the concerns specified in the Adjudicative Guidelines, and to collect feedback from cyber environment users about how participation affects their personal lives and work performance. Following this, it is necessary to learn how frequently people engage in activities of potential concern, understand if there are differences among users of different cyber environments (e.g., social networks vs. online games vs. explicitly anonymous environments, mobile activities, etc.), determine what those differences are, and generate recommendations for personnel security management.

Report II: Ethnographic Analysis of Second Life

As research progressed for Report I, it was determined that empirical research would be necessary to answer many important questions, and that the research

PART II: SCIENTIFIC CONTEXT AND RESEARCH GUIDANCE

would have different requirements than the present report. Report II uses an ethnographic approach to better understand Second Life, as available evidence indicated that its users might exhibit behaviors of personnel security concern. Ethnographic data collection methods capture the complexity of human experience. This entails watching people on their own territory, becoming immersed in their culture, building rapport to overcome disclosure barriers, and gathering information through observation, focus groups, and interviews (O'Reilly, 2004).

The Second Life ethnography was designed in coordination with a subcontractor who specializes in ethnographic methods and who has an established research presence in Second Life. Participants with characteristics similar to clearance holders (e.g., U.S. citizens, 18 or older, employed full-time, working in a professional environment, willing to accept an employment background check, etc.) were recruited, and then several methods were used to understand their Second Life activities and the impact on their real lives. Cyber activities were considered in context of the Adjudicative Guidelines, and real life spillover as related to health, relationships, functioning, and behavior in the workplace. Finally, the data were used to guide future research.

Prevalence of Risky Behaviors and Additional Recommendations

Research in progress seeks to determine the prevalence rates of behaviors of potential concern and generate best practice recommendations for investigators, adjudicators, personnel security managers, and policymakers. Some topics to be addressed include: (1) establishing the major points of awareness about the impact of cyber participation, (2) determining potential differences between types of environments, (3) proposing specific modifications to the Personnel Security Questionnaire (SF-86), (4) proposing specific changes to investigative methods and coverage, and (5) outlining considerations affecting the Adjudicative Guidelines.

Mobile and Pervasive Computing

Mobile and pervasive computing differs in important ways from traditional systems, and therefore requires special consideration. First, people are now vulnerable to exploitation by hostile parties while moving about, either because of their own actions or the capabilities of others. Second, some may grow so dependent on computers that heavy usage (e.g., many hours per day) becomes common. Finally, people who share constantly may find traditional interpersonal interaction to be difficult. In this vein, police have reported that domestic disturbance calls resulting from hostile or abusive text messages—with no physical contact—were once nonexistent but are now common. Furthermore, some couples refuse to interact face-to-face after particularly damaging messages are exchanged (Mitchell, 2010).

Conclusions

Personnel security measures are intended to prevent the loss of sensitive and valuable information, and loss can result either from the decisions of insiders to

PART II: SCIENTIFIC CONTEXT AND RESEARCH GUIDANCE

undermine this goal, or from the actions of hostile outside parties. Part I of this report introduced central cybersecurity concerns, with a primary focus on the social and cultural aspects of these risks. A great deal is known about external cyber threats, to include crime, terrorism, and counterintelligence. The necessary response is largely understood, and these topics have been addressed by other federal entities for some time. Part II outlined outside research on how changes to human behavior and society might affect the ability or willingness of insiders to protect information, but that the risks are not yet fully understood. The empirical studies conducted for this project, as summarized above, will together clarify cyberculture risks and potential ways for personnel security professionals to address and mitigate them.

The ultimate goal of the present project is to reach the point where personnel security policies, practices, and community awareness correspond to the psychological and cultural changes that have and are taking place. People today use computers to access more information, communicate more efficiently, and have more assistance than any generation in human history, so the impact is likely to be deep and have unexpected consequences. The first need is to raise awareness across the community about what can and does occur in cyberspace, ensure that the workforce is aware of how to responsibly and safely participate, and ensure that documents are updated to cover cyber activities that meet existing reporting requirements. The second need, and goal for moving forward, is to conduct research to establish fair and realistic coverage requirements for new topics, and to address situations where traditional assumptions about issues no longer make sense. Finally, because technology constantly evolves, new products and cultural changes must be periodically reviewed to ensure that personnel security activities are effective in protecting against the loss of controlled information.

REFERENCES

- AARP. (2010). *Social media and technology use among adults 50+*. Washington, DC: AARP.
- Aboujaoude, E., Koran, L. M., Gamel, N., Large, M. D., & Serpe, R. T. (2006). Potential markers for problematic internet use: A telephone survey of 2,513 adults. *CNS Spectrums*, 11, 750-755.
- Adams, W.L. (2008). UK couple to divorce over affair on Second Life. *Time Magazine*. Retrieved September 10, 2010, from <http://www.time.com/time/world/article/0,8599,1859231,00.html>.
- Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, December 29, 2005.
- Ali, S. (2010). *Small businesses join lawsuit against Yelp*. Retrieved January 6, 2011, from <http://blogs.wsj.com/digits/2010/03/17/small-businesses-join-lawsuit-against-yelp/>
- Albanesius, C. (2010). 'Call of Duty: Black Ops' Gamers Log 600M hours of play time. *PCMAG.COM*. Retrieved December 28, 2010, from <http://www.pcmag.com/article2/0,2817,2374762,00.asp>
- American Heritage® Dictionary of the English language. (2010). Retrieved June 11, 2010, from <http://education.yahoo.com/reference/dictionary/>
- American Psychiatric Association. (2000). *Diagnostic and statistical manual of mental disorders (4th ed.)*. Washington, DC.
- AmericasArmy.com (2010). *America's Army Official Website*. Retrieved June 7, 2010, from <http://www.americasarmy.com/>
- Anderson, K. J. (2001). Internet use among college students: An exploratory study. *Journal of American College Health*, 50, 1, 21-26.
- Armstrong, L., Phillips, J. G., & Saling, L. L. (2000). Potential determinants of heavier Internet usage. *International Journal of Human-Computer Studies*, 53, 537-550.
- Barak, A. (2010). *References related to the Internet & Psychology*. Retrieved June 23, 2010, from <http://construct.haifa.ac.il/~azy/refindx.htm>
- Bazelon, E. (2010). What really happened to Phoebe Prince? *Slate Magazine*. Retrieved July 30, 2010, from <http://www.slate.com/id/2260952/entry/2260953/>
- BBC News. (2005). *South Korean dies after games session*. Retrieved October 20, 2009, from <http://news.bbc.co.uk/2/hi/technology/4137782.stm>
- BBC News. (2010). *South Africa police hunt tweeting spy*. Retrieved September 15, 2010, from <http://www.bbc.co.uk/news/world-africa-11314555>

REFERENCES

- Beard, K. W., & Wolf, E. M. (2001). Modification in the proposed diagnostic criteria for Internet addiction. *Cyber Psychology and Behavior*, 4, 377-383.
- Bender, B. (2010). *Pentagon workers tied to child porn*. Retrieved July 30, 2010, from http://www.boston.com/news/nation/washington/articles/2010/07/23/pentagon_workers_tied_to_child_porn/
- Blair, D. (2010). Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, Denis C. Blair, Director of National Intelligence, February 2, 2010, 1-4. 111th Cong.
- Black, D. W., Belsare, G., & Schlosser, S. (1999). Clinical features, psychiatric comorbidity, and health-related quality of life in persons reporting compulsive computer use behavior. *The Journal of Clinical Psychiatry*, 60, 839-844.
- Block, J. J. (2008). Issues for DSM-IV: Internet addiction. *The American Journal of Psychiatry*, 165, 306-307.
- Boutin, P. (2010). *Mark Zuckerberg's personal mission: Convince the world to share*. Retrieved June 8, 2010, from <http://venturebeat.com/2010/05/20/facebook-privacy-mark-zuckerberg/>
- Brandon, J. (2007). *The top eight corporate sites in Second Life*. Retrieved June 9, 2010, from http://www.computerworld.com/s/article/9018238/The_top_eight_corporate_sites_in_Second_Life
- Brodkin, J. (2008). *IBM, Second Life create business-friendly virtual worlds*. Retrieved June 9, 2010, from <http://www.networkworld.com/news/2008/040308-ibm-second-life-virtual.html>
- Bush, R. (2009). *Reynard proposers' day IARPA-BAA-09-05 overview*. Retrieved July 31, 2009, from http://www.iarpa.gov/Reynard_Proposers_Day_Overview.pdf
- Businessweek. (2006). My virtual life. *Business Week*. Retrieved June 9, 2010, from http://www.businessweek.com/magazine/content/06_18/b3982001.htm
- Caplan, S. E. (2002). Problematic internet use and psychosocial well-being: Development of a theory-based cognitive-behavioral measurement instrument. *Computers in Human Behavior*, 18, 553-575.
- Caplan, S. E., Williams, D., & Yee, N. (2009). Problematic internet use and psychosocial well-being among MMO players. *Computers in Human Behavior*, 25, 1312-1319.
- Carnagey, N. L., Anderson, C. A., & Bushman, B. J. (2007). The effect of video game violence on physiological desensitization to real-life violence. *Journal of Experimental Social Psychology*, 43, 489-496.

- Carton, B. (2010). *I Can Stalk U: A 'Please Rob Me' for people who upload photos to Twitter*. Retrieved September 15, 2010, from http://legalblogwatch.typepad.com/legal_blog_watch/2010/09/i-can-stalk-u-a-please-rob-me-for-people-who-upload-photos-to-twitter.html
- Caspi, A., & Gorsky, P. (2006). Online deception: Prevalence, motivation, and emotion. *Cyber Psychology and Behavior*, 9, 54-59.
- Cavaglion, G. (2008). Voices of coping in an Italian self-help virtual community of cyberporn dependents. *Cyber Psychology and Behavior*, 11, 599-601.
- Chabinsky, S. R. (2009). Statement of Steven R. Chabinsky Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation before the Senate Judiciary Committee Subcommittee on Terrorism and Homeland Security at a hearing entitled "Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy Rights in Cyberspace." Presented November 17, 2009, 1-6, 111th Cong.
- Chang, D. (2010). *Augmented reality meets Facebook*. Retrieved May 17, 2010, from <http://asia.cnet.com/crave/2010/02/21/augmented-reality-meets-social-networking/>
- Chappell, D., Eatough, V., Davies, M. N. O., & Griffiths, M. (2006). *EverQuest – It's just a computer game right? An interpretative phenomenological analysis of online gaming addiction*. *International Journal of Mental Health and Addiction*, 4, 205-216.
- Chen, S. (2009). *The social network game boom*. Retrieved August 2, 2010, from http://www.gamasutra.com/view/feature/4009/the_social_network_game_boom.php
- Clark, D. (2010). *Second Life creator Linden Lab downsizes, morphs*. Retrieved September 6, 2010, from <http://blogs.wsj.com/digits/2010/06/10/second-life-creator-linden-lab-downsizes-morphs/>
- CNN. (2009). *Text messages of engineer in deadly train wreck detailed*. Retrieved December 22, 2010, from http://articles.cnn.com/2009-03-05/us/train.text_1_union-pacific-freight-train-locomotive-cell-phone?_s=PM:US
- Cohen, S., Doyle, W. J., Skoner, D. P., Rabin, B. S., & Gwaltney, J. M. (1997). Social ties and susceptibility to the common cold. *Journal of the American Medical Association*, 277, 1940-1944.
- Collins, L. (2008). Friend game: Behind the online hoax that led to a girl's suicide. *New Yorker*. Retrieved July 30, 2010, from http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_collins?currentPage=all
- Corbett, P. (2010). *Facebook demographics and statistics report June 2010 – Privacy concerns don't stop growth*. Retrieved December 22, 2010, from

REFERENCES

- <http://www.istrategylabs.com/2010/06/facebook-demographics-and-statistics-report-june-2010-%E2%80%93-privacy-concerns-dont-stop-growth/>
- Davis, R. A. (2001). A cognitive-behavioral model of pathological Internet use (PIU). *Computers in Human Behavior*, 17, 187-195.
- Davis, R. A., Flett, G. L., & Besser, A. (2002). Validation of a new scale for measuring problematic internet use: Implications for pre-employment screening. *Cyber Psychology and Behavior*, 5, 331-345.
- Department of Defense. (2006, June). *Nuclear Weapons Personnel Reliability Program (PRP) Regulation*. Washington, DC: Author.
- Diana, A. (2010). *Air Force Warns Against Location Based Sites*. Retrieved March 9, 2011, from http://www.informationweek.com/news/government/mobile/showArticle.jhtml?articleID=228300144&cid=RSSfeed_IWK_All
- Dill, K. E., & Dill, J.C. (1998). Video game violence: A review of the empirical literature. *Aggression and Violent Behavior*, 3, 407-428
- Ducheneaut, N., Yee, N., Nickell, E., & Moore, R. J. (2006). Building an MMO with mass appeal: A look at gameplay in World of Warcraft. *Games and Culture*, 1, 281-317.
- El Gazzar, S., Vitorovich, L., & Bender, R. (2011). 3rd UPDATE: Egypt Communications Cut As Protests Continue. *Wall Street Journal*. Retrieved January 28, 2011, from <http://online.wsj.com/article/BT-CO-20110128-709816.html>
- Elgan, M. (2010). *Are you a social networking mutant?* Retrieved June 7, 2010, from http://www.computerworld.com/s/article/9177694/Are_you_a_social_networking_mutant_?
- Executive Order 12968, *Access to Classified Information*, August 7, 1995.
- Flaherty, A. (2009, February 12). Congressman's online Twitter posts raise security concerns. *Boston Globe*. Retrieved September 10, 2009, from http://www.boston.com/news/nation/washington/articles/2009/02/12/congressmans_online_twitter_posts_raise_security_concerns/
- Fox News. (2006). *Chinese "Warcraft" game distributor sued over teen's suicide*. Retrieved October 8, 2009, from <http://www.foxnews.com/story/0,2933,195236,00.html>
- Fox News. (2007). *Boy collapses after playing "World of Warcraft" for 24 hours*. Retrieved October 8, 2009, from <http://www.foxnews.com/story/0,2933,453447,00.html>

REFERENCES

- Fox News. (2008). *Online game meetings sometimes end tragically, but phenomenon remains rare*. Retrieved October 9, 2009, from <http://www.foxnews.com/story/0,2933,316333,00.html>
- Francescani, C., & Kucharz, C. (2007). *Virtual child porn riles law enforcement*. Retrieved July 29, 2010, from <http://abcnews.go.com/TheLaw/story?id=3159871>
- Frontline. (2009). *Taking out the Taliban; Home for dinner*. Retrieved June 7, 2010, from <http://www.pbs.org/wgbh/pages/frontline/digitalnation/waging-war/remote-control-war/taking-out-the-taliban-home-for-dinner.html>
- Gentile, D. A., Lynch, P. J., Linder, J. R., & Walsh, D. A. (2004). The effects of violent video game habits on adolescent hostility, aggressive behaviors, and school performance. *Journal of Adolescence*, 27, 5-22.
- Google. (2010). Retrieved May 17, 2010, from <http://www.google.com/mobile/goggles/#landmark>
- Greenfield, D. N., & Davis, R. A. (2002). Lost in cyberspace: The web @ work. *Cyber Psychology and Behavior*, 5, 347-353.
- Gross, D. (2010). *The Facebook games that millions love (and hate)*. Retrieved August 2, 2010, from <http://www.cnn.com/2010/TECH/02/23/facebook.games/index.html>
- Hachman, M. (2010). f8: Facebook touts 'Open Graph,' Connects with smaller sites. *PCMag.COM*. Retrieved June 16, 2010, from <http://www.pcmag.com/article2/0,2817,2362920,00.asp>
- Hawkey, L. C., Thisted, R. A., & Cacioppo, J. T. (2009). Loneliness predicts reduced physical activity: Cross-sectional & longitudinal analyses. *Health Psychology*, 28, 354-363.
- Henthorn, D. (2010). *Ohio state flash mob goes viral: Link to video*. Retrieved May 18, 2010, from http://www.associatedcontent.com/article/2973592/ohio_state_flash_mob_goes_viral_link.html?cat=7
- Herbig, K. L. (2008). *Changes in espionage by Americans: 1947-2007*. Monterey, CA: Defense Personnel Security Research Center.
- Hersh, S. M. (2004). Torture at Abu Ghraib. *The New Yorker*. Retrieved September 6, 2010, from http://www.newyorker.com/archive/2004/05/10/040510fa_fact
- Hopkins. C. (2010). *Second Life economy at record high*. Retrieved June 11, 2010, from http://www.readwriteweb.com/archives/second_life_economy_at_record_high.php

REFERENCES

- IACP. (2010). *Developing a Cybervetting Strategy for Law Enforcement*. Alexandria, VA: International Association of Chiefs of Police.
- Immordino-Yang, M. H., McColl, A., Damasio, H., & Damasio, A. (2009). Neural correlates of admiration and compassion. *Proceedings of the National Academy of Sciences*, 106, 8021-8026.
- Ionescu, D. (2010). Geolocation 101: How it works, the apps, and your privacy. *PC World*. Retrieved May 17, 2010, from http://www.pcworld.com/article/192803/geolo.html?tk=rss_news
- Ivory, J. D., & Kalyanaraman, S. (2007). The effects of technological advancement and violent content in video games on players' feelings of presence, involvement, physiological arousal, and aggression. *Journal of Communication*, 57, 532-555.
- Kelkar, K. (2010). *Flash mobs flood the city on Valentine's Day*. Retrieved May 17, 2010, from <http://www.sfexaminer.com/local/Flash-mobs-flood-The-City-on-Valentines-day-84356747.html>
- Kim, J., LaRose, R., & Peng, W. (2009). Loneliness as the cause and the effect of problematic Internet use: The relationships between Internet use and psychological well being. *Cyber Psychology and Behavior*, 12, 451-455.
- King, S. A. (1999). Internet gambling and pornography: Illustrative examples of the psychological consequences of communication anarchy. *Cyber Psychology and Behavior*, 2, 175-184.
- Kirkpatrick, M. (2006). *Metaverse breached: Second Life customer database hacked*. Retrieved January 11, 2011, from <http://techcrunch.com/2006/09/08/metaverse-breached-second-life-customer-database-hacked/>
- Kirkpatrick, M. (2010). *Facebook's Zuckerberg says the age of privacy is over*. Retrieved May 17, 2010, from http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php
- Konijn, E. A., Bijvank, M. N., & Bushman, B. J. (2007). I wish I were a warrior: The role of wishful identification in the effects of violent video games on aggression in adolescent boys. *Developmental Psychology*, 43, 1038-1044.
- Kraut, R., Patterson, M., Lundmark, V., Kiesler, S., Mukopadhyay, T., & Scherlis, W. (1998). Internet paradox: A social technology that reduces social involvement and psychological well-being? *American Psychologist*, 53, 1017-1031.
- Leung, L. (2002). Loneliness, self-disclosure, and ICQ ("I Seek You") use. *Cyber Psychology and Behavior*, 5, 241-251.
- Li, Q. (2006). Cyberbullying in schools: A research of gender differences. *School Psychology International*, 27, 157-170.

- Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior*, 23, 1777-1791.
- Linden Lab. (2008). *Second life virtual economy demographic summary information through November 2008*. Retrieved August 3, 2009, from http://static-secondlife-com.s3.amazonaws.com/economy/stats_200811.xls
- Lipowicz, A. (2010). *vGov for feds aims to be a more engaging online environment*. Retrieved July 27, 2010, from http://fcw.com/articles/2010/07/12/feat-qanda-paulette-robinson-ndu-vgov.aspx?sc_lang=en
- Lund, R., Christensen, U., Holstein, B. E., Due, P., & Osler, M. (2006). Influence of marital history over two and three generations on early death. A longitudinal study of Danish men born in 1953. *Journal of Epidemiology and Community Health*, 60, 496-501.
- Mafiawarstips.com (2010). *The basics of Mafia wars*. Retrieved May 18, 2010, from www.mafiawarstips.com/Guide/TheBasics.html
- Maldives Mission (2010). *Maldives virtual embassy*. Retrieved September 3, 2010, from <http://maldivesmission.ch/index.php?id=65>
- Marines. (2009). *Immediate ban of internet social networking sites (SNS) on Marine Corps enterprise network (MCEN) NIPRNET*. Retrieved January 20, 2011, from <http://www.marines.mil/news/messages/pages/maradmin0458-09.aspx>
- Marines. (2010). *Responsible and effective use of internet-based capabilities*. Retrieved January 20, 2011, from <http://www.marines.mil/news/messages/Pages/MARADMIN181-10.aspx>
- McKeon, M. (2010). *The evolution of privacy on Facebook*. Retrieved August 2, 2010, from <http://mattmckeon.com/facebook-privacy/>
- McKenna, K. Y. A., & Bargh, J. A. (2000). Plan 9 from cyberspace: The implications of the internet for personality and social psychology. *Personality and Social Psychology Review*, 4, 57-75.
- McMillan, R. (2011). Man used Facebook to try to blackmail girl for porn. *PC World*. Retrieved February 4, 2011, from http://www.pcworld.com/article/218582/Man_Used_Facebook_to_Try_to_Blackmail_Girl_for_Porn.html?tk=rss_news
- Meerkerk, G. J. (2007). *Pwned by the internet: Explorative research into the causes and consequences of compulsive internet use*. Rotterdam: IVO.
- Mehdizadeh, S. (2010). Self-presentation 2.0: Narcissism and self-esteem on Facebook. *Cyberpsychology, Behavior, and Social Networking*, 13, 357-364.
- Mitchell, R. L. (2010). *Cop: Texting plays rising role in domestic disturbances*. Retrieved September 15, 2010, from

REFERENCES

- http://blogs.computerworld.com/16940/cop_texting_plays_rising_role_in_domestic_disturbances
- Morahan-Martin, J., & Schumacher, P. (2000). Incidence and correlates of pathological Internet use among college students. *Computer in Human Behavior*, 16, 13-29.
- Morrison, C. M., & Gore, H. (2010). The relationship between excessive Internet use and depression: A questionnaire-based study of 1,319 young people and adults. *Psychopathology*, 43, 121-126.
- MSNBC.com. (2007). *Hey parents, leave online gaming to the kids*. Retrieved November 9, 2009, from http://today.msnbc.msn.com/id/19855372/ns/technology_and_science-tech_and_gadgets
- Nalwa, K., & Anand, A. P. (2003). Internet addiction in students: A cause of concern. *Cyber Psychology and Behavior*, 6, 653-656.
- NCIS. (2010). *Cyber*. Retrieved December 17, 2010, from <http://www.ncis.navy.mil/CoreMissions/cyber/Pages/default.aspx>
- Ng, B. D., & Wiemer-Hastings, P. (2005). Addiction to the internet and online gaming. *Cyber Psychology and Behavior*, 8, 110-114.
- The Nielsen Company. (2010). *Social networks/blogs now account for one in every four and a half minutes online*. Retrieved July 6, 2010, from http://blog.nielsen.com/nielsenwire/online_mobile/social-media-accounts-for-22-percent-of-time-online/
- Nino, T. (2010). *Second Life statistical charts*. Retrieved June 11, 2010, from <http://dwellonit.taterunino.net/sl-statistical-charts/>
- O'Reilly, K. (2004). *Ethnographic methods*. New York, NY: Routledge.
- Padilla-Walker, L. M., Nelson, L. J., Carroll, J. S., & Jensen, A. C. (2009). More than a just a game: Video game and internet use during emerging adulthood. *Journal of Youth and Adolescence*. Retrieved October 30, 2009, from <http://www.springerlink.com/content/w487673k5415k142/fulltext.pdf>
- Parrish, K. (2010). *Blizzard cracks down erotic role-playing in WoW*. Retrieved December 13, 2010, from <http://www.tomshardware.com/news/World-of-Warcraft-MMO-MMORPG,11020.html>
- Paul, I. (2010). The Facebook data torrent debacle: Q&A. *PC World*. Retrieved August 2, 2010, from http://www.pcworld.com/article/202167/The_Facebook_Data_Torrent_Download_QA.html?tk=rss_news
- Pew Research Center (2010). *Older adults and social media: Social networking use among those ages 50 and older nearly doubled over the past year*. Retrieved

- September 6, 2010, from <http://pewinternet.org/Reports/2010/Older-Adults-and-Social-Media.aspx>
- Reuters. (2007). *UPDATE 3 - Linden Lab outlaws Second Life gambling*. Retrieved June 9, 2010, from <http://secondlife.reuters.com/stories/2007/07/26/linden-lab-outlaws-second-life-gambling/>
- Reuters. (2008). *Ageplay sim eyes new grid*. Retrieved June 10, 2010, from <http://secondlife.reuters.com/stories/2008/03/11/ageplay-sim-eyes-new-grid/index.html>
- Rideout, V. J., Foehr, U. G., & Roberts, D. F. (2010). *Generation M2: Media in the lives of 8- to 18-year-olds*. Retrieved September 6, 2010, from <http://www.kff.org/entmedia/8010.cfm>
- Riley, D. (2007). *You're not in the USSR any more: Estonia opens an embassy in Second Life*. Retrieved July 14, 2010, from <http://techcrunch.com/2007/12/05/youre-not-in-the-ussr-any-more-estonia-opens-an-embassy-in-second-life/>
- Rinckey, G. (2009). *Commentary: Social sites risk security clearance*. Retrieved November 17, 2009, from <http://federaltimes.va.newsmemory.com>
- Riva, G. (2002). The sociocognitive psychology of computer-mediated communication: The present and future of technology-based interactions. *CyberPsychology & Behavior*, 5, 581-598.
- Rosenwald, M. S. (2010). *Second Life's virtual money can become real-life cash*. Retrieved July 29, 2010, from <http://www.washingtonpost.com/wp-dyn/content/article/2010/03/07/AR2010030703524.html?hpid=topnews>
- Samuels, A. (2007). *Virtual marketers have second thoughts about Second Life*. Retrieved June 9, 2010, from <http://articles.latimes.com/2007/jul/14/business/fi-secondlife14>
- Shapira, N. A., Goldsmith, T. D., Keck, P. E., Khosla, U. M., & McElroy, S. L. (2000). Psychiatric features of individuals with problematic internet use. *Journal of Affective Disorders* 57, 267-272.
- Shapira, N. A., Lessig, M. C., Goldsmith, T. D., Szabo, S. T., Lazoritz, M., Gold, M. S., et al. (2003). Problematic internet use: Proposed classification and diagnostic criteria. *Depression and Anxiety*, 17, 207-216.
- Sheridan, M. (2010). *100 teens turn snowball fight into violent flash mob outside Philadelphia Macy's store*. Retrieved May 17, 2010, from http://www.nydailynews.com/news/national/2010/02/17/2010-02-17_100_teens_turn_snowball_fight_into_violent_flash_mob_outside_philadelphia_macys.html
- Sigman, A. (2009). Well connected? The biological implications of "social networking." *Biologist*, 56, 14-20.

REFERENCES

- Simmons, C. (2007). *Sweden opens virtual embassy 3D-style*. Retrieved September 3, 2010, from <http://www.sweden.se/eng/Home/Lifestyle/Reading/Second-Life/>
- Slatalla, M. (2009). *Caught in the deceit of the web*. Retrieved September 6, 2010, from <http://www.nytimes.com/2009/08/13/fashion/13spy.html>.
- Smith, A. (2010). *Mobile access 2010*. Retrieved July 7, 2010, from <http://www.pewinternet.org/Reports/2010/Mobile-Access-2010.aspx>
- Smith, J.R. (2010). *Would you want a digital footprint from birth?* Retrieved October 7, 2010, from <http://jrsmith.blog.avg.com/2010/10/would-you-want-a-digital-footprint-from-birth.html>
- Smith, P., Mahdavi, J., Carvalho, M., & Tippett, N. (2006, July). An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying. *Research Brief, Brief No: RBX03-06*.
- Snow, G. (2010). *Statement before the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security Washington, D.C.* Retrieved December 17, 2010, from <http://www.fbi.gov/news/testimony/the-fbi2019s-efforts-to-combat-cyber-crime-on-social-networking-sites>
- Steel, E. (2010). A web pioneer profiles users by name. *Wall Street Journal*. Retrieved January 11, 2011, from <http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html>
- Steinberg, S. (2010). *Apple game center: The Facebook of mobile gaming?* Retrieved July 6, 2010, from <http://www.cnn.com/2010/TECH/gaming.gadgets/07/05/apple.game.center.steinberg/index.html>
- Stone, B. (2010). *The children of cyberspace: Old fogies by their 20s*. Retrieved June 3, 2010, from <http://www.nytimes.com/2010/01/10/weekinreview/10stone.html?scp=1&sq=technology%20generation%20gap&st=cse>
- Subrahmanyam, K., & Greenfield, P. (2008, Spring). Online communication and adolescent relationships. *The Future of Children*, 18, 119-146. Retrieved June 21, 2010, from <http://www.jstor.org/stable/20053122>
- Suler, J. (2004). The online disinhibition effect. *Cyber Psychology and Behavior*, 7, 321-326.
- Sussman, B. (2007). *Teachers, college students lead a Second Life*. Retrieved June 9, 2010, from http://www.usatoday.com/news/education/2007-08-01-second-life_N.htm
- Terdiman, D. (2006). *Phony kids, virtual sex*. Retrieved August 5, 2009, from http://news.cnet.com/Phony-kids,-virtual-sex/2100-1043_3-6060132.html

REFERENCES

- Terdiman, D. (2008). *Banks banned in 'Second Life.'* Retrieved June 9, 2010, from http://news.cnet.com/8301-13772_3-9845886-52.html?tag=mncol;txt
- Timpane, J. (2011). *Arab world shaken by the power of Twitter and Facebook.* Retrieved January 28, 2011, from http://articles.philly.com/2011-01-27/news/27051558_1_social-media-facebook-page-twitter-and-facebook
- VNUnet News. (2002). *Second gamer dies after massive binge.* Retrieved October 6, 2009, from <http://www.v3.co.uk/vnunet/news/2120472/second-gamer-dies-massive-binge>
- Waterman, S. (2010). *Fictitious femme fatale fooled cybersecurity.* Retrieved July 28, 2010, from <http://www.washingtontimes.com/news/2010/jul/18/fictitious-femme-fatale-fooled-cybersecurity/>
- Weaver, J. B., Mays, D., Weaver, S. S., Kannenberg, W., Hopkins, G. L., Eroglu, D., & Bernhardt, J. M. (2009). Health-risk correlates of video-game playing among adults. *American Journal of Preventative Medicine*, 37, 299-305.
- White, J. (2005). *It's a video game, and an Army recruiter.* Retrieved June 7, 2010, from <http://www.washingtonpost.com/wp-dyn/content/article/2005/05/26/AR2005052601505.html>
- Williams, D., Yee, N., & Caplan, S. E. (2008). Who plays, how much, and why? A behavioral player census of virtual world. *Journal of Computer-Mediated Communication*, 13, 993-1018.
- Woollacott, E. (2010). *Second Life to become browser-based as Linden Lab restructures.* Retrieved June 10, 2010, from <http://www.tgdaily.com/games-and-entertainment-features/50158-second-life-to-become-browser-based-as-linden-restructures>
- Yee, N. (2004). *The Daedalus gateway: The psychology of MMORPGs.* Retrieved June 8, 2010, from http://www.nickyyee.com/daedalus/gateway_addiction.html
- Young, J. (2010). *After frustrations in Second Life, colleges look to new virtual worlds.* Retrieved June 9, 2010, from <http://chronicle.com/article/After-Frustrations-in-Second/64137/>
- Young, K. S. (1998). Internet addiction: The emergence of a new clinical disorder. *Cyber Psychology and Behavior*, 1, 237-244.
- Young, K. S. (2008). Internet sex addiction risk factors, stages of development, and treatment. *American Behavioral Scientist*, 52, 21-37.
- Young K. S., & Rogers, R. C. (1998). The relationship between depression and Internet addiction. *Cyber Psychology and Behavior*, 1, 25-28.
- Zani, D. (2010). *Lightsaber flash mob attacks an innocent shopping mall.* Retrieved May 17, 2010, from <http://www.cinemablend.com/new/Lightsaber-Flash-Mob-Attacks-An-Innocent-Shopping-Mall-17095.html>

REFERENCES

- Zavis, A. (2009). *Judge tentatively dismisses case in MySpace hoax that led to teenage girl's suicide*. Retrieved July 30, 2010, from <http://latimesblogs.latimes.com/lanow/2009/07/myspace-sentencing.html>
- Zhao, S., Grasmuck, S., & Martin, J. (2008). Identity construction on Facebook: Digital empowerment in anchored relationships. *Computers in Human Behavior*, 24, 1816-1836.